

JOINT INTEROPERABILITY AND ENGINEERING ORGANIZATION

System Administration Manual

rev 0

January 15, 1997

GCCS-SAM-2.2

**SYSTEM ADMINISTRATION MANUAL
GCCS VERSION 2.2**

SUBMITTED BY:
Intae Kim
Major, USAF
Chief Engineer

APPROVED BY:
Ellis K. Conoley
Colonel, USAF
Program Manager, GCCS

TABLE OF CONTENTS

<u>Section</u>	<u>Page</u>
1. SCOPE	1-1
1.1 Overview of this Manual	1-1
2. LIST OF DOCUMENTS	2-1
2.1 Mail Administration Documents	2-1
2.2 Domain Name Service (DNS) Administration Documents	2-1
2.3 Other Documents	2-1
3. SEGMENT INSTALLATION	3-1
3.1 Overview	3-1
3.2 Setting Up Network Segment Installation Servers	3-1
3.3 Using the Segment Installer	3-2
3.4 Using the Remote Installer	3-5
3.4.1 Using Remote Install for the Pull Operation	3-6
3.4.2 Using Remote Install for the Push Operation	3-7
3.4.2.1 Remote Install Push Example	3-8
3.4.2.2 Remote Install Install/De-install Example	3-9
3.4.3 Configuring a Repository Site for Pull Operation	3-10
4. TELECONFERENCING	4-1
4.1 Introduction	4-1
4.1.1 Internet Relay Chat (IRC)	4-1
4.1.2 Newsgroups (Usenet News)	4-1
4.1.3 World Wide Web	4-2
4.2 Internet Relay Chat (IRC)	4-3
4.2.1 How to Install the Server	4-4
4.2.2 Administering the IRC Server and the IRC Network	4-6
4.3 Newsgroups	4-6
4.3.1 Installation Instructions for NEWSS (Internet News Server Segment)	4-6
4.3.2 How to Start and Stop the Server	4-8
4.3.3 How to Throttle (Pause) the Server	4-8
4.3.4 How to Get the Server to Re-Read its Configuration Files	4-9
4.3.5 How to Add/Remove Newsfeeds (Neighboring Servers)	4-10
4.3.6 Creating a Newsgroup	4-10
4.3.6.1 Establishing a Newsgroup Across the GCCS Network	4-10
4.3.7 Adding, Deleting, and Modifying Users' Access to News	4-11
4.3.8 How to Support Multiple Newsgroup Access List Maintainers	4-13
4.3.9 How to Remove a Newsgroup	4-13
4.3.10 Archiving a Newsgroup	4-14
4.3.10.1 Why Archive a Newsgroup	4-14
4.3.10.2 How to Archive a Newsgroup	4-15
4.3.10.3 How to Access Archived Articles	4-15
4.3.10.4 How to Read NEWSS Man Pages	4-15

TABLE OF CONTENTS (cont.)

<u>Section</u>	<u>Page</u>
4.3.11 What to Do if Disaster Strikes	4-15
4.3.12 News Make Group	4-17
4.4.1 Netsite Installation	4-18
4.4.2 httpd Installation	4-18
5. DOMAIN NAME SERVICE ADMINISTRATION	5-1
5.1 Overview	5-1
5.2 References	5-1
5.3 Pre-Installation Tasks	5-2
5.4 Installing the Primary Name Server	5-3
5.5 Secondary Name Server Setup	5-8
5.6 Set Up the Remaining Hosts on the Network	5-8
5.7 Debugging Hints	5-9
5.8 Updating the Name Server Database	5-9
5.9 Solaris 2.3 Specifics	5-10
6. NIS+ ADMINISTRATION	6-1
6.1 Overview of NIS+	6-1
6.1.1 An Explanation of the Basic NIS+ Objects	6-1
6.1.1.1 Directory Objects	6-1
6.1.1.2 Table Objects	6-1
6.1.1.3 Group Objects	6-2
6.1.1.4 Link Objects	6-2
6.2 Debugging NIS+	6-2
6.2.1 Authentication Problems	6-2
6.2.2 Examining NIS+ Tables	6-3
6.2.3 Using Snoop	6-3
6.2.4 Performance Problems	6-4
6.2.5 GCCS Version 2.2 Information	6-4
6.3 Common How-Tos	6-4
6.3.1 How to Prepare Your Site for NIS+	6-4
6.3.2 How to Set Up a Root NIS+ Master	6-5
6.3.3 How to Set Up a NIS+ Client	6-6
6.3.4 How to Set Up a Root NIS+ Replica	6-6
6.3.5 How to Set Up a Subdomain NIS+ Master	6-7
6.3.6 How to Set Up a Subdomain NIS+ Replica	6-7
6.3.7 How to Configure the Root Server for an IP Address Change	6-8
6.3.8 How to Add a User to the Admin Group	6-8
6.3.9 How to Change a NIS+ User Password	6-9
6.3.10 How to Change a NIS+ root password	6-9
6.3.11 How to Administer NIS+ Credentials	6-10
6.3.12 How to Administer NIS+ Groups	6-10
6.3.13 How to Administer NIS+ Tables	6-11
6.3.14 How to Examine NIS+ tables	6-12
6.3.15 How to Modify NIS+ Tables	6-12
6.3.16 How to Regularly Administer NIS+	6-14

TABLE OF CONTENTS (cont.)

<u>Section</u>	<u>Page</u>
6.3.17	How to Remove NIS+ 6-14
6.3.18	How to define the printer table in NIS+ 6-14
6.4	Some Frequently Asked Questions 6-15
6.4.1	Miscellaneous Questions 6-15
6.4.2	NIS+ Setup Problems 6-16
6.4.3	User Log-in Problems 6-16
6.4.4	NIS+ Lookup Problems 6-17
6.5	References 6-17
6.5.1	Important Man Pages 6-17
6.5.2	Sunsolve Documents 6-18
6.5.2.1	FAQs 6-18
6.5.2.2	Infodocs 6-18
6.5.2.3	SRDBs 6-18
6.5.3	Sun Educational Services 6-18
6.5.4	Solaris Documentation 6-19
6.5.5	Third Party Documentation 6-19
6.5.6	RFCs 6-19
6.6	Supportability 6-19
6.7	Additional Support 6-19
7.	MAIL ADMINISTRATION 7-1
7.1	Introduction 7-1
7.2	Mail Administration Files 7-2
8.	PRINTER ADMINISTRATION 8-1
8.1	Scope 8-1
8.2	Installing NeWSprint on Print Servers 8-1
8.3	GCCS Desktop Printer Concept of Operations 8-3
8.3.1	Network Printing Support 8-3
8.3.1.1	Printer Administrator 8-4
8.3.1.2	User Print Manager 8-4
8.3.2	Remote (Dial-Up) Printing Support 8-5
8.3.2.1	Remote Print Server Configuration 8-5
8.3.2.2	Session Control 8-5
8.3.2.3	Remote Print Software 8-6
8.3.3	GCCS Printer Administration User's Guide 8-6
8.3.3.1	Adding A printer to a Print Server 8-6
8.3.3.2	Adding Remote Printer 8-7
8.3.3.3	Modifying a GCCS Printer Entry 8-7
8.3.3.4	Removing a Printer from the Network 8-7
8.3.3.5	Selecting a GCCS System Default Printer 8-8
8.3.3.6	Getting Current Printer Status 8-8
8.3.3.7	Updating Print Clients on the Network 8-8
8.3.3.8	Terminating the GCCS Printer Admin Manager 8-8
8.3.4	The Current Printer File 8-8
8.3.5	The Printer Table 8-9
8.4	Configuring a System to Print Remotely 8-10

TABLE OF CONTENTS (cont.)

<u>Section</u>	<u>Page</u>
8.4.1	Configuring Solaris 8-10
8.4.2	Configuring HP-UX 8-11
9.	USER ACCOUNT ADMINISTRATION 9-1
9.1	Basics about DBUSER 6.0 9-1
9.1.1	DBUSER Scripts 9-1
9.1.2	Log Files 9-1
9.1.3	DBUSER Interface 9-2
9.2	Adding User Accounts to GCCS 9-2
9.2.1	Creating User Accounts 9-2
9.2.2	Customizing Profiles 9-3
9.3	Executing the 'grant_user' DBUSER Script 9-4
9.3.1	Working in SINGLE USER Mode 9-4
9.3.2	Working in MULTIPLE USER Mode 9-5
9.4	Executing the 'revoke_user' DBUSER Script 9-7
9.4.1	Working in SINGLE USER Mode 9-7
9.4.2	Working in MULTIPLE USER Mode 9-8
9.5	Notes Relating to specific GCCS Segments 9-9
9.5.1	JOPEs 9-10
9.5.2	RDA 9-10
9.5.3	PDR USER 9-10
9.5.4	JOPEs PDRPT 9-10
9.5.5	GSORTS 9-10
9.5.6	LOGSAFE 9-10
9.5.7	JEPES 9-11
9.5.8	MEPES 9-11
9.5.9	AIRFIELD 9-11
9.5.10	RFA DATABASE 9-11
9.5.11	TCCESI 9-11
9.5.12	NPG 9-11
9.5.13	GTN (SMINT) DATABASE 9-12
9.5.14	FRAS 9-12
9.5.15	GRIS 9-12
9.5.16	RPI 9-12
9.5.17	EVAC 9-12
10.	SOFTWARE LICENSE ADMINISTRATION 10-1
10.1	Applix License Setup Procedures 10-1
10.2	JDISS License Setup Procedures 10-2
10.2.1	Client/Server Relationship 10-2
10.2.2	License File Procedures for JDISS Version 2.0.3 10-2
10.2.3	Procedures for Machines Currently Running Older Version That Upgrade v2.0.3. 10-3
10.3	NeWSprint License Setup Procedures 10-3
10.3.1	NeWSprint Version 2.0 Setup Procedure 10-3
10.3.1.1	Acquiring a Font Password 10-3
10.3.2	Upgrading a License for NeWSprint V2.0 to V.2.1 10-3

TABLE OF CONTENTS (cont.)

<u>Section</u>	<u>Page</u>
10.3.3 NeWSprint Version 2.5 License Setup Procedures	10-4
11. SPARCSTORAGE ARRAY ADMINISTRATION	11-1
11.1 Overview	11-1
11.2 GCCS Configuration Considerations	11-1
11.3 Identifying a Failed Disk	11-3
11.3.1 Command Line Interface Techniques	11-3
11.3.2 Graphical User Interface Techniques	11-5
11.4 Disk Replacement Scenarios	11-7
11.4.1 Overview of Procedures	11-7
11.4.2 Hot Spare Disk Operations	11-8
11.4.3 Volume Operations (Non-Mirrored Disk Configurations) . . .	11-9
11.5 Disk Removal and Installation	11-9
11.5.1 Physical Disk Removal	11-10
11.5.2 Physical Disk Installation	11-11
11.6 Restoring VM Configurations	11-12
11.6.1 Restoring Hot Spare Configuration	11-12
11.6.2 Restoring Non-Hot Spare Configuration	11-14
12. GSORTS ADMINISTRATION	12-1
12.1 Downloading GSORTS Database	12-1
12.2 Using CDROM Maps	12-2
13. HARDWARE ADMINISTRATION	13-1
13.1 Fiber Distributed Data Interface	13-1
13.1.1 Procedures for Installing FDDI Interface Software	13-1
13.1.2 3800 Router Configuration	13-3
13.2 Synoptics 300S Intelligent HUB Introduction	13-3
13.2.1 Purpose of the HUB	13-4
13.2.2 Inventory	13-4
13.2.3 Configuration of 3800 Router Module	13-6
13.2.4 Configuration of 3313A Ethernet Network Management Module	13-7
14. CONFIGURING PCs TO DISPLAY DESKTOP	14-1
14.1 X-Package Installation	14-1
14.1.1 Preparation for Installation	14-1
14.1.2 Screen Setups	14-1
14.1.3 XoftWare/32	14-1
14.1.4 PC-Xware	14-3
14.1.5 eXceed 4 for Windows	14-5
14.1.6 Reflection-X	14-7
14.1.7 XVision	14-9
15. INFORMATION MANAGEMENT SUBSYSTEM/REFERENCE FILE MANAGER (IMS/RFM) ADMINISTRATION	15-1
15.1 IMS Admin Tool	15-1

TABLE OF CONTENTS (cont.)

<u>Section</u>	<u>Page</u>
15.1.1 Who Can Run the IMS Admin Tool	15-1
15.1.2 How to Recover the Original IMS Configuration	15-1
15.2 RFM	15-1
15.2.1 Who Can Run the RFM Admin Tool	15-1
15.2.2 How to Recover the Original RFM Configuration	15-1
16. CHANGING IP ADDRESSES AND HOST NAMES	16-1
16.1 Changing IP Addresses on SPARCstations	16-1
16.2 Changing the Host Name of a SPARCstation	16-2
16.3 Changes Required to NIS+ and DNS when Changing Host Names and IP Addresses	16-3
16.4 Changing IP Address and/or Host Name on Sybase Server	16-4
17. UPS ADMINISTRATION	17-1
17.1 Related Documents	17-1
17.2 Hardware Installation	17-1
17.3 OnliSafe Powerware Software Installation	17-3
18. EXECUTIVE MANAGER OPERATIONS	18-1
18.1 Introduction	18-1
18.2 User Account Maintenance	18-2
18.2.1 Security Manager Activation	18-3
18.2.2 Security Manager Termination	18-3
18.2.3 Security Main Window	18-4
18.2.4 User Account Maintenance Tasks	18-4
18.2.5 Group Maintenance Tasks	18-7
18.2.6 Audit Monitoring	18-9
18.2.6.1 Setting DB Audit Parameters	18-9
18.2.6.2 Viewing UNIX Audit Logs	18-10
18.2.6.3 Viewing Database Audit Logs	18-10
18.2.7 Updating Security Caveats	18-11
18.2.8 Setting Access Parameters	18-11
18.3 System Profile Maintenance	18-12
18.3.1 Profile Description	18-12
18.3.1.1 Profile Manager Activation	18-12
18.3.1.2 Profile Manager Termination	18-14
18.3.2 Profile Manager Menus	18-14
18.3.3 System Profile Maintenance Tasks	18-14
18.3.3.1 Viewing Users and Profiles	18-14
18.3.3.2 Profile Attribute Maintenance	18-16
18.3.4 User Profile Maintenance	18-23
18.3.4.1 Creating a New User Profile	18-23
18.3.4.2 Delete a User Profile	18-23
18.3.4.3 Modifying a User Profile	18-23
18.3.5 Launch List Maintenance	18-24
18.3.5.1 Modifying a User Launch List	18-24

TABLE OF CONTENTS (cont.)

<u>Section</u>	<u>Page</u>
18.3.6 Profiles Display Order	18-24
18.4 System Assign Roles Maintenance	18-25
18.4.1 Role Manager Activation	18-25
18.4.2 Role Manager Termination	18-26
18.4.3 Role Manager Menus	18-26
18.4.4 Adding a Role to Account Group: Security Admin	18-26
18.4.5 Adding a Role to Account Group: System Admin	18-30
18.4.6 Adding a Role to Account Group: GCCS Operator	18-31
18.4.7 Deleting a Role from an Account Group	18-31
18.4.8 Edit an Existing Role for an Account Group	18-31
18.4.9 Duplicate a Role from an Existing User	18-32
18.4.10 Print a Role of a User(s)	18-32
18.4.11 Exit the Role Manager Main Menu	18-32
18.5 The Monitor Program	18-32
18.6 The Control Manager Program	18-32
 19. ANSWERBOOK ADMINISTRATION	 19-1
 20. DISK DUPLICATION PROCEDURES	 20-1
20.1 Lessons Learned	20-1
20.2 Initial Conditions	20-1
20.3 Procedure	20-1
 APPENDIX A. ORACLE RDBMS OVERVIEW	 A-1
A.1 Understanding the ORACLE Database	A-1
A.1.1 Database Structure	A-2
A.1.1.1 Physical Database Structure	A-2
A.1.1.2 Logical Database Structure	A-3
A.1.2 Database User Access and Privileges	A-4
A.1.3 ORACLE Database Startup and Shutdown	A-6
A.1.4 Database Recovery and Backup	A-7
A.1.4.1 Database Recovery	A-7
A.1.4.2 Database Backup	A-8
A.1.4.2.1 Off-Line Database Backups	A-8
A.1.4.2.2 On-Line Database Backups	A-10
A.1.5 Accessing ORACLE DBA Utilities	A-11
A.1.5.1 Database Startup	A-12
A.1.5.2 Database Shutdown	A-12
A.1.6 Accessing SQL*PLUS	A-13
A.1.7 Passwords	A-14
A.1.8 Maintaining SQL*Net	A-15
A.1.9 SQL*Net V1	A-15
A.1.10 SQL*Net V2	A-15
A.1.11 ORACLE Network Manager	A-17
A.1.12 Full System Export	A-18
A.1.13 Creating New User Tables	A-18
A.1.14 Correcting Database Fragmentation	A-19

TABLE OF CONTENTS (cont.)

<u>Section</u>	<u>Page</u>
A.2	Determining Free Space in a Tablespace A-19
A.3	Database Monitor Routines A-19
 APPENDIX B. ENGINEERING EVALUATION OF PC X-SERVERS AND PC TCP/IP	
	PRODUCTS B-1
B.1	Introduction B-1
B.2	Evaluation Criteria and Product Evaluated B-1
B.2.1	PC X-Servers B-1
B.2.1.1	Criteria B-1
B.2.1.2	Products Evaluated B-1
B.2.2	TCP/IP Products B-2
B.2.2.1	Criteria B-2
B.2.2.2	Products Evaluated B-2
B.3	PC X-Server Products B-2
B.3.1	Summary of Findings B-2
B.3.2	Product Reviews B-3
B.3.2.1	eXceed 4 for Windows B-3
B.3.2.1.1	Product Overview B-3
B.3.2.1.2	Product Description B-3
B.3.2.1.3	Product Evaluation B-4
B.3.2.2	XoftWare/32 for Windows B-6
B.3.2.2.1	Product Overview B-6
B.3.2.2.2	Product Description B-6
B.3.2.2.3	Product Evaluation B-7
B.3.2.3	PC-Xware B-9
B.3.2.3.1	Product Overview B-9
B.3.2.3.2	Product Description B-9
B.3.2.3.3	Product Evaluation B-11
B.3.2.4	Reflection-X B-12
B.3.2.4.1	Product Overview B-12
B.3.2.4.2	Product Description B-12
B.3.2.4.3	Product Evaluation B-13
B.4	TCP/IP Candidate Products B-15
B.4.1	Summary of Findings B-15
B.4.2	Product Reviews B-15
B.4.2.1	Chameleon/NFS B-15
B.4.2.1.1	Product Overview B-15
B.4.2.1.2	Product Description B-15
B.4.2.1.3	Product Evaluation B-18
B.4.2.2	Microsoft VxD 32 TCP/IP B-19
B.4.2.2.1	Product Overview B-19
B.4.2.2.2	Product Description B-20
B.4.2.2.3	Product Evaluation B-20
B.5	PC X-Server Attributes/Requirements/Features B-21
B.6	PCs-to-UNIX Connections: an Overview B-24
B.6.1	Desktop to Enterprise Connections B-24
B.6.2	TCP/IP Driver Implementations B-24

TABLE OF CONTENTS (cont.)

<u>Section</u>	<u>Page</u>
B.6.3 TSR Implementation	B-24
B.6.4 DLL Implementation	B-25
B.6.5 The VxD Alternative	B-25
B.6.6 Microsoft's Recommendation for the Future: VxD	B-26
B.6.7 Summary	B-26
 APPENDIX C. MSQL DATABASE ADMINISTRATION GUIDE	 C-1
C.1 Introduction	C-1
C.2 Mini SQL Specification	C-1
C.2.1 The Create Clause	C-1
C.2.2 The Drop Clause	C-2
C.2.3 The Insert Clause	C-2
C.2.4 The Select Clause	C-2
C.2.5 The Update Clause	C-4
C.3 The mSQL Terminal Monitor	C-4
C.4 mSQL Database Administration	C-5
C.5 mSQL Schema Viewer	C-5
C.6 mSQL Database Dumper	C-5
C.7 Access Control	C-6
C.8 Drop_buttons	C-7
 APPENDIX D. SITE DOMAIN NAMES	 D-1
 APPENDIX E. ESTABLISHING THE ACCOUNT FOR USER <i>news</i>	 E-1
 APPENDIX F. SYSTEM BACKUP AND RECOVERY	 F-1
F.1 Scope	F-1
F.2 System Backup Strategy	F-1
F.3 System Backup Segment Description	F-1
F.4 Specific Data Backed Up	F-2
F.4.1 NIS+ Server	F-2
F.4.2 Sybase Server	F-2
F.4.3 Executive Manager Server	F-2
F.4.4 DNS Server	F-3
F.4.5 All GCCS Systems	F-3
F.5 Recovery	F-3
F.5.1 NIS+	F-3
F.5.1.1 NIS+ Database Corrupted Recovery Procedures	F-3
F.5.1.2 NIS+ Server Rebuilding Procedures	F-4
F.5.2 DNS	F-6
F.5.2.1 Restoring DNS Database on Original DNS Server	F-6
F.5.2.2 Building a New DNS Server Using the Backed Up DNS Database	F-7
F.5.3 Sybase	F-8
F.5.3.1 Restoration of Sybase Database	F-8
F.5.3.2 Rebuilding of Sybase Database Server	F-8
F.5.3.2.1 Setting up Sybase Raw Disk Partitions	F-8

TABLE OF CONTENTS (cont.)

<u>Section</u>	<u>Page</u>
F.5.3.2.2 Setting up Sybase File System	F-9
F.5.3.2.3 Installing and Initializing Sybase	F-9
F.5.4 Executive Manager Recovery	F-11
F.5.4.1 Building a New Executive Manager Server	F-11
F.5.4.2 Modifying All Other GCCS Platforms to Use New EM Server	F-13
F.5.5 Recovering the Network Installer TOC	F-14
F.5.6 Crash Recovery	F-15

Figures

<u>Figure</u>	<u>Page</u>
3-1. Remote Install Window	3-6
3-2. Select Segments Screen	3-7
14-1. XoftWare/32 Screen Captures	14-3
14-2. PC-Xware Screen Captures	14-3
14-3. eXceed 4 Windows Screen Captures	14-5
14-4. Reflection X Screen Captures	14-7
14-5. XVision Screen Captures	14-9
17-1. UPS Front Panel Controls and Indicators	17-2
18-1. System Administrator's Desktop Menu Structure	18-2
18-2. Security Manager's Desktop Menu Structure	18-4
18-3. Security Manager Main Window	18-5
18-4. Security Manager Menu Structure	18-6
18-5. Profile Manager Main Window	18-13
18-6. Profile Manager Menu Structure	18-15
18-7. Role Manager Main Window	18-25
18-8. Role Manager Menu Structure	18-27
18-9. Add Role Main Menu	18-29
18-10. Security Admin Role Header	18-30
18-11. System Admin Account Group	18-31
18-12. GCCS Operator Account Group	18-31
18-13. Monitor Menu	18-33
18-14. Control Manager Menu	18-33
 A-1. The ORACLE Physical Database Structure	 A-2
A-2. Role/Privilege Setup	A-5

Tables

<u>Table</u>	<u>Page</u>
4-1. Teleconferencing Applications	4-1
4.1.3-1. WIN Teleconferencing Replacement Segments	4-2
13-1. Synoptics 3000S Hub Components	13-5
13-2. Configuration of 3800 Router	13-6
13-3. Configuration of 3313A Ethernet NMM	13-7
19-1. AnswerBook Installation Options	19-3
 B-1. Evaluation Criteria of eXceed 4 Windows	 B-5
B-2. Evaluation Criteria of XoftWare/32 for Windows	B-8
B-3. Evaluation Criteria of PC-Xware	B-11
B-4. Evaluation Criteria of Reflection-X	B-14
B-5. TCP/IP for PC Attributes	B-18
B-6. PC X-Server Attributes and Requirements	B-21
B-7. PC X-Server Features of the Candidate Products	B-22

SECTION 1. SCOPE

The Global Command and Control System (GCCS) is an Automated Information System (AIS) supporting the Department of Defense (DoD). GCCS is producing, integrating, and fielding new hardware and software components designed to provide the Joint Planning and Execution Community (JPEC) with new technology and functionality. GCCS system integration emphasizes use of commercial off-the-shelf (COTS) products, and merges the capabilities of a modern Local Area Network (LAN), UNIX-based client/server architecture, desktop-style Graphical User Interface (GUI), and a Relational Database Management System (RDBMS).

GCCS is intended to help Joint operation planners satisfy their deliberate and crisis planning responsibilities via access to a useful, user-tested, integrated set of analytic tools and flexible data transfer capabilities. The GCCS client/server architecture provides a firm foundation for linking external systems and GCCS components, permitting easy access to applications, and faster, more reliable, data transfers within a secure environment. At the heart of GCCS is a large database and application server connected to a LAN. The GCCS LAN interconnects the GCCS server with a variety of workstations (DOS and Microsoft Windows PCs, Macintosh, UNIX, and other X-Windows clients) that run associated software and application packages. The GCCS LAN will also connect with Wide Area Networks (WANs) supporting standard LAN design.

The GCCS architecture is specifically designed with flexibility and COTS standardization to allow interconnection with new networks and systems as they are deployed. This architecture will easily adapt to and assimilate new applications and functions.

GCCS is designed with the user in mind; powerful and flexible, yet fully functional. However, achieving these goals involves a complex system design, with a regular and effective technical, "behind the scenes" system administration (SA) activity. Consequently, trained SA personnel are absolutely essential to the satisfactory operation of the GCCS system resources at each site. This SA Manual provides technical system administration guidance for DoD sites receiving GCCS Version 2.2

1.1 Overview of this Manual

This manual:

- Provides guidance to sites on establishing SA positions, prerequisites, and qualifications.
- Describes the responsibilities of the GCCS SA with reference to specific Sun Microsystems Corporation products. (SunOS 5.3 designates the operating system only. Solaris 2.3 designates the distributed computer environment software.)
- Provides guidance to GCCS SAs on executing their

responsibilities.

- Provides instructions to GCCS SAs on where to get further assistance.

This manual will not restate:

- Standard platform-specific (i.e., SunOS, HP-UX) documentation (each GCCS site will receive separately); or
- GCCS system and applications user documentation, BUT will address user-specific database issues.

SECTION 2. LIST OF DOCUMENTS

2.1 Mail Administration Documents

- a. *sendmail* - by Bryan Costales with Eric Allman & Neil Rickert, published by O'Reilly & Associates.
- b. *sendmail - An Internetwork Mail Router*, by Eric Allman (SMM-16)
- c. *sendmail - Installation and Operation Guide*, by Eric Allman (SMM-07)

Also useful are these Requests for Comments (RFC's):

RFC822 *Standard for the Format of ARPA-Internet Text Messages*
RFC821 *Simple Mail Transfer Protocol*
RFC819 *The Domain naming Convention for Internet User Applications*
RFC1123 *Requirements for Internet hosts - Application and Support.*

2.2 Domain Name Service (DNS) Administration Documents

Administrating NIS+ and DNS (Solaris Manual)

DNS and BIND (O'Reilly & Associates, Inc, Paul Albitz & Cricket Liu)

2.3 Other Documents

- *Airfields Software Users Manual*, 16 February 1995.
- *Airfields Software Center Operator Manual*, 16 February 1996.
- *ESI JOPES External System Interfaces (ESI) Software Users Manual*, 20 September 1996.
- *FRAS (Fuel Resource Analysis System) Software Users Manual*, 24 May 1996.
- *GCCS Automated Information System (AIS), Security Plan*, 23 January 1996.
- *GCCS Software Users Manual: JOPES Users Guide Update*, 15 May 1996.
- *Ad Hoc Query User Manual*, 28 June 1996.
- *GRIS System Administration*, 20 August 199.
- *GSORTS User's Guide*, 19 August 1994, Change 1, 30 June 1995.
- *HP NetMetrix Power Agent Users Guide (Volume 1, 2 and 3) Version*

4.5, 25 May 1995.

- *IMS/RFM User Handbook*, 11 March 1996.
- *JDISS System Administration Manual, JDISS Server v2.0.3 and Client v2.0.4/GCCS 2.1/2.2 w/Change 1*, 7 November 1996.
- *JDISS IPA Client v1.2.1 Installation & System Administration Manual, GCCS v2.1/2.2 w/Change 1*, 7 November 1996.
- *JDISS Installation Manual, Server Segment v2.0.3 and Client Segment v2.0.4/GCCS 2.1/2.2 w/Change 1*, 7 November 1996.
- *JOPES System Service Administration Manual*, 31 July 1996.
- *JOPES Core Database Maintenance Manual*, 16 February 1996.
- *MEPES (Medical Planning and Execution System) Users Manual (UM)*, 28 June 1996.
- *PREDEFINED Reports Users Manual*, 27 September 1996.
- *RDA (Requirements Development and Analysis) Build 2 Users Manual*, 7 June 1995.
- *TARGET Users Manual, v 2.2*, 29 December 1995.
- *TARGET v 2.2.2 System Administration Notes*, 9 August 1996.
- *Unified Build v3.0.1.6g System Administration Guide (change pages)*, 27 September 1996.

SECTION 3. SEGMENT INSTALLATION

3.1 Overview

In GCCS, all software is packaged in modules called software segments. An application may comprise one or more segments, depending upon its complexity and modularity. The segments are provided to the site on 4mm or 8mm tapes, via ftp over the SIPRNET, or can be installed remotely by a repository site (Operational Support Facility or CINC) using the Remote Installer. The segments are installed using the Segment Installer tool, which comes with the GCCS COE Kernel. It is available when the SA logs in as sysadmin.

3.2 Setting Up Network Segment Installation Servers

Network Segment Installation servers are GCCS platforms on which software segments can be loaded and stored. The Segment Installer can then use the Segment Installation servers to install applications on other platforms. This eliminates the need for using tapes to install segments and allows the SA to build several platforms simultaneously.

The Executive Manager server stores the Table of Contents for the Segment Installation servers in the directory `/h/data/global/SysAdm/toc_load`, which is mounted by all systems. The table of contents, `toc`, identifies the segments available on the network, and the platforms storing each segment. The actual segments are stored in the `/home2` directory on the Segment Installation server. The SA should insure that `/home2` has sufficient space to accommodate the required segments; if space is limited, the SA can set up separate platforms as Network Installation servers. The following are the steps for setting up a Segment Installation server:

- a. If, during the installation of the GCCS COE Kernel tape, the question:

"Is this going to be a Segment Installation Server? (y/n)[n]"

was answered "y" then go to Step c.

If the question was answered "n," and the site now wants to set the server up as a Segment Installation server, then go to Step b. before performing Step c.

- b. Add the following line in `/etc/dfs/dfstab`:

```
Share -F nfs -o anon=o /home2
```

and execute the following command:

```
/etc/share /home2
```

- c. Log in as sysadmin and select INSTALLATION SERVER from the SOFTWARE menu.
- d. If the tape drive from which you will be loading the software segments is locally attached, and is device 0, go to Step e. Otherwise, click the SELECT MEDIA button.
 1. If the tape drive is on another platform, select HOST under HOST and then click on the field next to NAME. Enter the name or the IP address of the remote platform. Select OTHER under DEVICE and then click on the field under OTHER. Enter the correct drive number, ensuring that the "b" option is used (e.g., /dev/rmt/0mbn).
 2. If the tape drive is locally attached, select **OTHER** under DEVICE and then click on the field under OTHER. Enter the correct drive number, ensuring that the "b" option is used (e.g., /dev/rmt/1mbn).
- e. Load the desired segment tape in the tape drive and select **READ TOC**.
- f. Use the cursor to highlight the segments to be loaded. Highlight as many as desired.
- g. Select **LOAD** to begin loading the selected segments. The segments will be installed in /home2 in the NET_SERVER directory. The Table of Contents will be stored in directory /h/data/global/SysAdm/toc_load.
- h. The Installation server will not load any segments after /home2 has reached 80 percent of its capacity. To override this constraint, position the cursor in the Segment Installer GUI, and press the right mouse button. Select **Disk Space Override** from the menu. A new window labeled "OVERRIDE DISK SPACE LIMITATIONS" will appear. Select the desired override (**90 percent** or **95 percent**) from this window and then **EXIT**. Continue loading segments after this.

To allow another platform to use the Segment Installation server, an .rhosts file must be created in the / directory. This file must have the host names of each platform in which the Segment Installation server will be used.

3.3 Using the Segment Installer

The segments are installed using the Segment Installer tool, which is a GUI that provides the following:

- Identification of which applications (segments) are loaded on your system.
- Identification of which applications (segments) are available on a tape or on a Segment Installation server.
- The capability to install and/or de-install applications (segments) on the system.

The Segment Installer installs software in the `/h` file system. When this file system is approximately 80 percent full, the Segment Installer will install software in `/home1`, followed by `/home2`, `/home3`, ..., `/home99`. The 80 percent constraint can be overridden by using the **Disk Space Override** feature of the Segment Installer.

The Segment Installer tool can be invoked directly by logging in as **sysadmin** and launching it via the icon or menu pick, or by the Remote Installer tool (RemoteInst), addressed in Section 3.4. To use the Segment Installer do the following:

- a. Log in as **sysadmin**.
- b. Position the cursor over the **SOFTWARE** menu pick and select **Segment Installer**, or position the cursor over the **Install** icon in the Launch Window and double-click. The Segment Installer GUI will appear after approximately 15 seconds.
- c. If loading from tape, and if the tape drive from which you will be loading the software segments is locally attached, and is device 0, go to Step e; otherwise click the **SELECT MEDIA** button. A "Checking Media" window will appear for approximately 30 seconds, sometimes longer. A window labeled "Select Media" will then appear.
- d. In the "Select Media" window execute one of the following:
 1. If you are going to use the Segment Installation server, select **NETWORK** under DEVICE and then select **OK**.
 2. If the tape drive is on another platform, select **HOST** under HOST and then click on the field next to NAME. Enter the name or the IP address of the remote platform. Select **OTHER** under DEVICE and then click on the field under OTHER. Enter the correct drive number, ensuring that the "b" option is used (e.g., `/dev/rmt/0mbn`).
 3. If the tape drive is locally attached, select **OTHER** under DEVICE and then click on the field under OTHER. Enter the correct drive number, ensuring that the "b"

option is used (e.g., `/dev/rmt/0mbn`).

- e. Load the segment tape in the tape drive and select **READ TOC**. If using the Segment Installation server, simply select **READ TOC**.
- f. The Segment Installer GUI will disappear, and a window containing an hourglass labeled "Checking Media" will be displayed. The "Checking Media" window will disappear and another hourglass window labeled "Busy" will be displayed, with a message "Reading Table of Contents."
- g. The Segment Installer GUI will reappear with a list of available segments displayed in the window labeled "Table of Contents." Segments already installed will have an asterisk. (The Table of Contents and the *SegDescrip* directory for each segment listed are stored in:

`/h/data/local/SysAdm/toc_load`, if loaded from tape, or in
`/h/data/global/SysAdm/toc_load` if network installed).
- h. To select a segment for installation, move the cursor to the segment to be installed and click once. The segment will be highlighted.

NOTE: It is possible to select more than one segment for installation at a time, but it is not recommended, especially for segments larger than 20 MB. Never install more than one application database segment at a time.

- i. To begin the install process, select the **Install** button. A window with an hourglass labeled "Installing Selected Segments" will appear in place of the Segment Installer GUI. The application and database segment tables located in Section 5 of the GCCS Implementation Procedures show approximately how long it takes to load each segment.
- j. After the segment is installed, the Segment Installer GUI will reappear with another window overlaid signifying that the segment was either successfully or unsuccessfully installed.
- k. If the segment was successfully installed, continue loading additional segments if required.
- l. If the segment did not install successfully, a warning will appear stating that an "error occurred while installing selected segment(s)." Click on **OK** to clear the warning and then select **STAT LOG** to determine why the segment(s) did not install.

The most common explanations for a segment not installing are:

- The required segments are not installed on the system.
- The segment is not JMCIS compatible.
- Insufficient disk space is available to install the segment.

To correct the "required segments not installed" problem, highlight the problem segment in the Table of Contents window, and select **REQUIRED**. Install any segments listed that are not currently installed. Also consult the Segment Dependency table in Section 5 of the *GCCS Implementation Procedures* for any additional dependencies. Pay particular attention to the version number of the required segments. If the version currently installed does not match the version specified for the required segments, the segment still may not install.

To correct the "not JMCIS compatible" problem, exit the Segment Installer and rewind the tape. After the tape is rewound, restart the Segment Installer and try again.

To correct the "insufficient disk space" problem, use the Disk Space Override feature of the Segment Installer (see Step n following).

- m. If a segment did not install successfully, but is listed in the "SEGMENTS CURRENTLY INSTALLED" window of the Segment Installer, it should be de-installed before attempting to re-install it.
- n. The Segment Installer will not load any segments after the available `/h` and `/home[1-99]` file systems have reach 80 percent of their capacity. To override this constraint, position the cursor in the Segment Installer GUI and press the right mouse button. Select **Disk Space Override** from the menu. A new window labeled "OVERRIDE DISK SPACE LIMITATIONS" will appear. Select the desired override (**90 percent** or **95 percent**) from this window and then **EXIT**. Continue loading segments after this.

3.4 Using the Remote Installer

The Remote Install (RemoteInst) function provides the following capabilities:

- It allows an operator at a remote site to "pull" software segment(s) from a repository site and load them in the remote site's Segment Installation server. The operator may also use RemoteInst to install the segment(s) on a platform after

they are pulled.

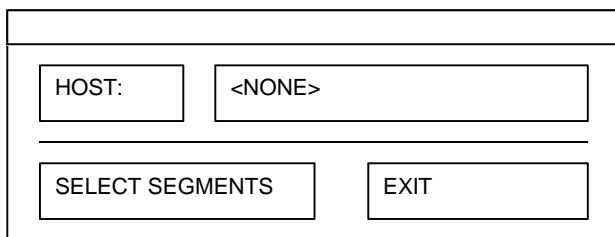
- It allows an operator at a repository site the ability to download or "push" software segments to other sites where they are loaded into the site's Segment Installation server. It also provides the operator at the repository site the ability to install or de-install segments on platforms at other sites.

3.4.1 Using Remote Install for the Pull Operation. The Pull operation consists of an operator at the remote site grabbing and transferring software segments, made up of segment install file(s) and shell scripts, from the repository site to the remote site. The Pull operation has a graphical user interface intended for ease of use.

NOTE: Prior to executing the following steps, the Remote Install segment must be installed.

To run the Remote Install in Pull mode, do the following:

- a. At the remote site, log onto a platform as **sysadmin**.
- b. Select **Remote Install** from the "Software" menu or double-click on the **Remote Install** icon. This brings up a window like that shown in Figure 3-1.



HOST: <NONE>	
SELECT SEGMENTS	EXIT

Figure 3-1. Remote Install Window

- c. Enter the name of the repository host in the text field containing the word "<NONE>".
- d. Select **SELECT SEGMENTS**. This will connect to the repository machine and bring up the screen shown in Figure 3-2, which contains a list of segments available for pulling from the repository site:

NOTE: If the repository site machine is not set up correctly, the following message will appear:

"No segments found on the specified host"

Consult Section 3.4.3 for instructions on configuring a repository site.

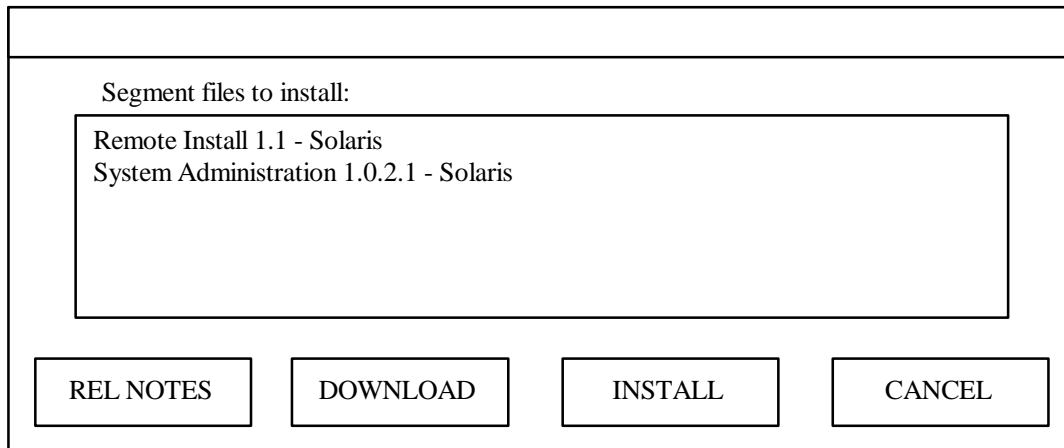


Figure 3-2. Select Segments Screen

- e. Select the segment(s) to be pulled by moving the mouse to the desired segment and clicking once. The segment(s) will be highlighted.
- f. To pull the segment and load it on the site's network Segment Installation server, select **DOWNLOAD**.
- g. To install the segment on the platform executing Remote Install, in addition to loading it on the network Segment Installation server, select **INSTALL**.
- h. Progress will be indicated by the following series of messages:
 - Transferring files
 - Formatting segments
 - Launching Installer (only if INSTALL was selected)
- i. If **INSTALL** was selected, the Segment Installer will appear after the segments are transferred. Follow the procedures in Section 3.3 to use the Segment Installer.

3.4.2 Using Remote Install for the Push Operation. The Push operation consists of an operator at the repository site (Operational Support Facility or CINC) sending the Segment Install File and shell

scripts from the repository site to the client (remote) site. The operator has the ability to load the segment on the remote site's Network Installation server (Segment Installation server) and install/de-install segments on the remote site's platforms. The Push operation uses only a command line interface, as follows:

```
RemoteInst [-p -l -i] <hostname> <segment install file>
```

Where:

-p indicates that the Remote Installer should only send the file across the network and load it on the Network Segment Installation server specified in **<hostname>** in the directory **/home2/NET_SERVER**. It does not install the segment on the remote site.

-i indicates that the tool should send the file and install the file on the Network Segment Installation server specified in **<hostname>**, and then launch the Segment Installer on the remote machine so the Remote Install operator can go ahead and install the segment.

-l indicates that the tool should launch the remote machine's Segment Installer so that it is displayed on the repository machine's display.

<hostname> is the host name or IP address of the machine at the remote site on which the segment will be installed. For option **-p** + **-i** host name must be the name of a Network Segment Installation server.

<segment install file> is the full path of the segment install file that is to be installed. Only one segment install file may be installed at a time.

3.4.2.1 Remote Install Push Example. The following is an example of a Push operation. In the example, a segment file named *RemoteInstall_1.1.tar*, located under */home10/ftp/pub/RemoteInstall* at the repository site, is installed on the remote site's Network Installation server machine, named *jdefest.jdef*, without launching the installer on the remote machine:

- a. **RemoteInst -p jdefest.jdef
/home10/ftp/pub/RemoteInst/RemoteInstall_1.1.tar**
- b. The operator will then be prompted for valid user ID and password on the machine to which the segment is being pushed. Enter **root** or **sysadmin** as a valid user ID.
- c. After entering the correct user ID and password, the operator would see a series of messages similar to the following:

Checking remote system type...
Attempting to get free space from remote machine...
Free Disk Space on Remote Machine == 255428 KB

Installing Segment File
[/home10/ftp/pub/RemoteInst/RemoteInst_1.1.tar]

This can take a while - - please be patient.

Sending file: RemoteInst_1.1.tar
100% 0 =====> 2447360 bytes. ETA: 0:00
2447360 bytes sent in 2.19 seconds, 1.06 MB/s.
Sending file: AddToNetTOC
100% 0 =====> 7415 bytes. ETA: 0:00
7415 bytes sent in 0.03 seconds, 276.14 kB/s

Formatting segment on remote machine... [Network Installation
Server]

Expanding the segment file (this may take a while)...[Extracting
the tar file]

Adding new segment to the table of contents...

Adding segment to the network installer...

Cleaning up ... Please be patient

Network install completed

*** Remote Install Completed ***

3.4.2.2 Remote Install Install/De-install Example. To de-install and/or install segments on a remote machine, Remote Install provides the ability to launch the remote machine's Segment Installer on the repository machine's display. This uses a command line interface, as follows:

- a. **RemoteInst -l 199.114.208.77**
- b. The operator will then be prompted for valid user ID and password on the remote machine on which the Segment Installer is being launched.
- c. The Remote Install tool will transfer a file to configure the account for using the Segment Installer. Finally, the installer will be launched on the remote display. During this process the operator will see the following messages:

Checking remote system type...
Attempting to get free space from remote machine...
User sysadmin logged in.
Sending file: LaunchInstaller

```
100% 0 ===== 1396 bytes. ETA: 0:00
1396 bytes sent in 0.05 seconds, 24.98 kB/s.
Launching Segment Installer on 121.0.0.125:0.0
```

- d. At this point, the Segment Installer will appear on the repository machine's display. Follow the procedures in Section 3.3 to use the Segment Installer to install/deinstall segments on the remote machine.

3.4.3 Configuring a Repository Site for Pull Operation. For the Pull operation to work, the repository site needs to be configured properly. First, the Pull works by using anonymous ftp. Refer to the manual pages for "ftpd" for information on setting up anonymous ftp. Once anonymous ftp is configured, some additional files need to be added under the *ftp* home directory:

~ftp/pub/SegFiles

This file contains data on the segment install files. It is a plain text file that contains one line for each segment install file on the system. The line contains three fields that are separated by colons, as:

<description>:<relative segment file path>:<relative release notes path>

Where:

<description>: is the description that will appear on the Remote Install window when a user attaches to the repository site using the Pull operation (Section 3.4.1). The field should contain at a minimum the segment name, the version number, the machine type, and the file size.

<relative segment file path>: is the path and name of the segment install file [local tar file].

<relative release notes path>: is an optional field that indicates the path and file name of the release notes files.

A valid *SegFiles* file would look like the following:

```
Remote Install 1.1:/pub/RemoteInst/RemoteInst_1.1.tar: /pub/RelNotes/RemoteInst.RN
JMTK 1.0 for Solaris:/pub/JMTK/JMTK_1.0.tar:/pub/JMTK/JMTK_1.0.RN
System Administration 1.0.2.1:/pub/SysAdm/SysAdm.1.0.2.1.tar:
```

~ftp/pub/ShellScripts/AddToNetTOC

~ftp/pub/ShellScripts/LaunchInstaller

The two files in bold face above are distributed with the Remote Install segment. They are shell scripts that load the pulled segment(s) on the Network Installation server [*AddToNetTOC*] and launch the Segment Installer [*LaunchInstaller*]. They can be found under

/h/RemoteInst/progs after the Remote Installer segment has been installed.

NOTE: All segment install files must reside under the *~ftp/pub* directory for the Pull function of Remote Install to work.

SECTION 4. TELECONFERENCING

4.1 Introduction

Teleconferencing consists of three applications. These applications were acquired from public domain sources and from commercial vendors. Only minor modifications have been made to make them appropriate for use on the SIPRNET. The changes were specifically in the areas of need-to-know and access restriction. Table 4-1 lists the applications.

Table 4-1. Teleconferencing Applications

Name	Remarks
Internet Relay Chat (IRC)	Interactive, Non-persistent, Text-based
Usenet News (NewsGroups)	Non-real-time Interactive, Short Term Persistency, Text-Based, also known as Newsgroups
World Wide Web	Limited Interactivity, Long Term Persistence, Text and Binary Capability

4.1.1 Internet Relay Chat (IRC)

The first application, IRC, is a real-time interactive conferencing tool. Messages input to a conference are made visible to other participants in the conference within seconds. It is non-persistent; there is no mechanism for reviewing old messages. However, it is possible for each user to log a conference session (create a text file containing a copy of every message that appeared in a conference while that user was connected to the conference). Its functionality is similar that of a telephone conference call.

4.1.2 Newsgroups (Usenet News)

The second application is Usenet News, known as Newsgroups. This application is a version of the well-known Newsgroups on the Internet. Users run client software termed a *newsreader*, which downloads articles from a news server. The client software receives the news articles that are current at the time the client logged onto the particular Newsgroup. If articles arrive after the user has attached to the server, the user will not be made aware of them until the user re-connects. This, combined with the fact that it can take tens of minutes for a news article to propagate to all servers in the network, makes News less interactive than IRC. The articles that are posted to newsgroups are almost always text files, i.e., they do not carry the type of control characters normally found in a word processor and they do not carry binary graphical files. Newsgroup servers connect to each other and automatically pass news articles among themselves, making it possible for a subscriber to receive news articles while connected to his or her

local News server.

4.1.3 World Wide Web

The third application of the Teleconferencing replacement functionality is the World Wide Web. This application provides the ability to move large files of any type using an intuitive graphical interface. This is not an interactive application; the author of a document makes it available on "the Web," and other users download the document for viewing and/or printing. This application provides to the user the ability to publish and download formatted word processor files and binary graphical files such as maps and pictures. The ability of web *browsers* (web client software) to utilize external programs to view or process documents does not commit the GCCS community to any particular binary format for formatted text or graphical data.

Each of these applications follows the client-server model and is composed of multiple GCCS segments. These segments are identified in Table 4.1.3-1.

Table 4.1.3-1. WIN Teleconferencing Replacement Segments

Application Segment	Program Name	Prefix	Interdependencies
Internet Chat (IRC)			
Server:	ircd	IRCS	
Client:	Zircon (GUI chatter)	IRCC	
	irc (Text based chatter)	IRCC	
NewsGroups			
Server:	innd	NEWSS	PERL
	perl (scripting language)	PERL	
World Wide Web			
Servers:	httpd	HTTPD	
	Netsite	WEBSV	
Client:	Netscape	WEBBr	
	Home Page Generator	WEBPg	PERL

NOTES: 1) Netsite and Netscape are commercial products; licenses are being obtained by DISA for their use.

If Netsite and Netscape licenses are not available, then Netsite is replaced by httpd and Netscape is replaced by MOSAIC.

2) While the PERL segment is nominally part of the Newsgroups and World Wide Web segments, it can be used by other GCCS applications.

4.2 Internet Relay Chat (IRC)

Internet Relay Chat (IRC) is a chatter-style program that allows multiple users to participate in conferences. The segment is similar to the "Comm" portion of WIN Teleconferencing. It is implemented as a network of IRC servers. Users interact with IRC via IRC clients. There are two clients available to users; a low-bandwidth, text-based client, named *irc*, and a GUI client named *Zircon*. A user invokes an IRC client and directs the client to connect to a server. Once connected, the user participates in conferences/ conversations by joining specific channels. A channel may be thought of as a topic of discussion, or even as a conference. By joining a channel, the user will then receive all messages sent to that channel. Further, when the user inputs a message to the channel, the message is forwarded to all other clients on the same channel (including clients attached to other servers in the network).

The IRC server software is *ircd*. It is a UNIX daemon that runs continuously on a server platform. Each site is expected to have at least one IRC server running at all times. This software server does not require a site to procure an additional hardware server, but may be loaded on a currently available hardware server. The application *ircd* is written in C, and utilizes sockets for interprocess communication. The default port is 6667.

IRC is non-persistent in that messages are not automatically saved. It is very interactive. When a user types a message on his screen, it is very quickly transmitted to all other servers on the network and then from those servers to all users currently connected to that conference. However, when a message is sent while a user is not connected, that user will not be able to see that message. Features supported include private channels (users not on a channel cannot see who is on that channel), secret channels (users not on channel cannot even detect that the channel exists), keyed channels (users must know a password to join a channel), invitation-only channels (a channel operator must send a user an invitation before that user can join the channel), and moderated channels (channel operators can provide/remove permission to individuals to input messages to the channel).

Zircon is an X-based package providing an elegant GUI interface to IRC. It is written in the Tcl scripting language, and thus requires that Tcl, Tk, and Tcl-dp be present on the machine from which it is executed. Tcl, Tk and Tcl-dp are included. Features include sidebar conversations (two-way conversations invisible to others), pop-up channel displays (iconified channel windows will restore themselves when a message arrives on the channel), and queries as to the identity of other users.

Internet Relay Chat consists of a series of servers connected in a logical network.

4.2.1 How to Install the Server. IRC comprises two segments. *IRCS* is the IRC Server segment. It contains the application named *ircd*. It requires at least a Sparc 20, although it requires very little disk space. *IRCC* is the IRC Client segment. It contains two IRC clients; *irc* (an ASCII - based client) and *Zircon* (an X-based client). The client software should be installed on any machine at which users will be expected to use IRC. Both *IRCS* and *IRCC* contain binaries for both Sun and HP platforms. The installation scripts remove the inappropriate binaries.

The Installation Script will prompt the installer to answer the following five questions. Question 4 is particularly critical in that it discusses the information that must be provided to other site administrators (and what information they must provide to you).

Q1: Is this site a hub node or a leaf node?

The first question concerns whether the server in question will be a hub node or a leaf node. A hub is a server that communicates with multiple other servers. A leaf node is a server that communicates with only one other server. Table 4.3 identifies sites as either leaf nodes or hub nodes.

Q2: What is the server name?

The PostInstall script attempts to determine the sites server machine's name and IP address. It is recommended to use the machine's fully-qualified name (*machine.domain.name*, where *domain.name* is the DNS domain name).

Q3: Enter administrative info

The installer is asked the name of the facility, descriptive information about the server, and a point-of-contact (POC) for the server. This information will be made available to clients attaching to the server (a client can issue an ADMIN command, which returns this information). Since this information is not used internally by IRC, the installer can respond in any way to these questions. However, we strongly recommend that the installer make the entries informative. The descriptive

information about the server is particularly useful if the site is installing multiple servers. The POC information should include the name, telephone number, and e-mail address of the system administrator in charge of maintaining the IRC server.

Q4: Entering the IRC Network neighbors

This section configures the server to communicate with its neighbors in the IRC network. The following information is required.

- The machine name and/or IP address that the neighboring server will run on
- The name of the server itself (should be the same as the name of the machine)
- The password that the server must provide to gain access to that neighbor
- Whether the neighbor is a hub or a leaf.

Q5: Establishing operator access

An IRC operator (IRCOp) is a user who has operator privileges on the IRC network. These privileges include the ability to "squit" servers (remove the link between those servers, resulting in a partitioned network), "connect" servers, "kill" users (kicking them off of a server), etc. The IRC Server configuration file allows one to specify the nickname(s) and password(s) of the IRC operator, as well as specifying which client machine(s) a user can be connected from and still become an operator. Leaf nodes do not require that there be any operators, and should not allow operators unless there is an administrator who is responsible for maintaining IRC at that site. Hub nodes require knowledgeable operators. Those servers should allow operators to connect to the server from clients running on the server machine, and should not allow operators to connect from other machines.

SPECIAL NOTE ON THE INSTALLATION:

A site administrator can edit the IRC server configuration file with any text editor. The file is:

`/h/COTS/IRCS/lib/ircd/ircd.conf`

Its format is intended to be human-readable. This configuration file has no comments, but the file:

`/h/COTS/IRCS/skel/ircd.conf`

is a fully-commented skeleton ircd configuration file that will help one understand the syntax of *ircd.conf*.

4.2.2 Administering the IRC Server and the IRC Network

There is little work to be done to administer an IRC server or IRC network as a whole. System Administrators will modify connections as necessitated by failures in other servers and communications links.

4.3 Newsgroups

4.3.1 Installation Instructions for NEWSS (Internet News Server Segment)

Installing the Internet News Server segment (NEWSS) requires that the installer respond to six questions posed by the PostInstall software. Some amount of planning is required before installing NEWSS. Please read this entire document before beginning the installation.

Question #2 (Q2 below) asks for the name of the directory in which the News spool should reside. The "News spool" is the directory tree into which all incoming News articles are stored. Since this can grow to a truly tremendous size, it is strongly recommended that the spool be located on a separate disk partition from `/h/COTS/NEWSS/lib`. Choose a partition for the spool such that no critical application will crash if the partition becomes full. The history files (located in `/h/COTS/NEWSS/lib`) can also grow to be quite large, although they should remain under 10 megabytes.

Q1 -- E-mail address:

The first installation question requests that the site enter the e-mail addresses of the individuals entrusted with the responsibility of maintaining the News server. These person(s) will most likely be the System Administrator(s). In any case, the News server will, at times, send e-mail to the user `news 0`. This e-mail will contain important information with respect to administering the News server. This section of the PostInstall allows the SA to specify the users to whom this e-mail should be forwarded. It will continue to prompt for e-mail addresses until the SA responds with a carriage return (<CR>), at which point it will prompt to confirm the list of e-mail addresses. If the SA does not confirm, the e-mail addresses previously entered will be dropped and the site will have to start over in Q1.

Q2 -- Parent directory of news spool:

When News articles arrive at the server, they are stored into the spool directory. Due to the potentially high volume of news traffic, it is possible that the partition that stores the spool directory will become full. It is thus important that the spool be placed in a partition that can become full without crashing the

server or causing undue problems with server applications. One such application is the News server itself; if the spool is placed on the same partition as `/h/COTS/NEWSS/lib`, then when the partition becomes full, no lock files can be created in `/h/COTS/NEWSS/lib`. The impact of this is that "ctlinnd" cannot be run (it utilizes lock files in `/h/COTS/NEWSS/lib`), and thus the News administrators cannot manually purge News articles (which would release disk space). Note that if there is already a News spool in the specified directory, the site will be offered the opportunity to use that News spool, rather than copying the install spool over it.

Q3 -- The name of the current domain:

Enter the DNS domain for the server.

Q4 -- The name of your organization:

Every News posting includes, as part of its header, the "organization" of the individual posting the article. Enter a line of text (≤ 64 characters, including spaces) describing the site. Examples would be "FORSCOM" or "Central Command."

Q5 -- Load a previously saved configuration

The DE-INSTALL script for NEWSS supports saving the site's configuration files (the contents of `NEWSS/lib`) in a tar file in `/h/data/global`. The purpose of this is to prevent users from losing a configuration that may have evolved over an extended period of time and be difficult to re-create (*especially* `nntp.access`). If a site loads an old configuration, the next two questions are skipped.

Q6 -- Establish the (News Server) network

This is the screen in which the site specifies its neighboring servers (the servers which feed articles to the site's server and which, in turn, are fed by the site's server). This is where the information exchanged with the News administrators at neighboring sites is used. Since NEWSS is based upon machine-to-machine connectivity (as opposed to site-to-site), the installer must know which machine at each neighboring site will be the News server. Also, the installer must exchange News passwords with neighboring site installers. These passwords are used to authenticate server connections. When associating passwords with server connections, use a different password for each neighboring server (do not use the same password for a neighbor that neighbor is using for your server). For each neighbor, four inputs are required:

- the server machine's fully qualified name

(*machine.domain.name*) or IP address

- the server's "pathname" (the name it appends to an article's path—usually the fully qualified machine name)
- the password the site's neighbor must provide for the site to allow a connection
- the password that the site's server must provide to its neighbor when connecting to it

For security reasons, all passwords should be unique. The input process will continue until the site responds to "Neighbor's IP address or fully-qualified name :" with <CR>.

Q7 -- Create the Server's Access Control List

The News server software only accepts client connections from users who have entries in the access control file (*nnrp.access*). The site need not enter all of its users at this point in time. Enter one or two for testing purposes, and then modify (or write a script to modify) *NEWSS/lib/nnrp.access* later on.

4.3.2 How to Start and Stop the Server. If *innd* (the news server) is not running on a machine, it must be started by *root*. To start the server, execute the program:

```
/h/COTS/NEWSS/progs/rc.news
```

To stop the server, user *root* should enter the command:

```
/h/COTS/NEWSS/progs/ctlinnd shutdown "reason"
```

This is a UNIX command that will stop the process running the server.

4.3.3 How to Throttle (Pause) the Server. There will be times when a News administrator wants to pause the server (stop it from receiving articles, etc.) without terminating the server. Examples of activities an administrator may wish to perform while the server is paused are: editing the active file, re-building the history database, and backing up or modifying the News spool. The program *ctlinnd* (control *innd*) is used to pause the server as follows:

```
/h/COTS/NEWSS/progs/newsbin/ctlinnd pause "reason"
```

"reason" is a string that indicates why the server is being paused. This string is stored in the *innd* log files for future reference.

To resume normal server operation:

```
/h/COTS/NEWSS/progs/newsbin/ctlinnd go "reason"
```

"reason" must either be the same reason as was used to throttle the server, or the empty string (two quotes with no characters in between).

The manual (man) pages entry that covers these operations are (see 4.3.14 for instructions on reading the man pages):

```
man ctlinnd (8)
```

4.3.4 How to Get the Server to Re-Read its Configuration Files. The *ctlinnd* program with the command "reload" is used to reload the configuration files into memory. The format of the command is:

```
/h/COTS/NEWSS/progs/newsbin/ctlinnd reload "what reason"
```

where "what" is one of the following: *all*, *history*, *hosts.nntp*, *active*, and *overview.fmt*. "Reason" is a string (enclosed by quotes if it contains space characters) explaining why the reload was performed. Below is a list explaining the result of each "what" specification.

all	Reload all configuration files, close and re-open the history database
history	Close and re-open the history database.
hosts.nntp	Re-read the <i>hosts.nntp</i> file - specifies neighboring servers and the password they must provide to connect to the site.
active, newsfeeds	Both the active and the newsfeeds files are reloaded for either command. The active file specifies which newsgroups are active at this server, and the newsfeeds file specifies which servers the site feeds news to, which newsgroups are fed to those servers, and how the site connects to those servers.
overview.fmt	Reload the <i>overview.fmt</i> file, which specifies the format of the overview database. GCCS News administrators should never have to do this, as there should never be a need for a site to customize their <i>overview.fmt</i> file.

Note that there is no way to reload the *inn.conf* file. This should not be an issue, as the "path" variable is the only part of *inn.conf* used by *inn*.

The manual (man) pages that cover these operations are:

```
ctlinnd (8)
hosts.nntp (5)
overview.fmt (5)
active (5)
history (5)
innd (8).
```

4.3.5 How to Add/Remove Newsfeeds (Neighboring Servers). Adding new neighbors to the site's server or removing existing neighbors involves editing four files in */h/COTS/NEWSS/lib*:

- *hosts.nntp*
- *newsfeeds*
- *nntpsendctl*
- *passwd.nntp*.

The file *hosts.nntp* lists the machines (name or IP address) that feed news to this server, plus the password those servers must supply to be allowed to connect to this server. The file *newsfeeds* specifies where news articles get forwarded to and how they get forwarded. The file *nntpsendctl* is the control file for the program *nntpsend*, which is the program that actually transmits articles from this site to the neighboring servers. Finally, *passwd.nntp* is the file that specifies the passwords the server must supply to connect to its neighbors. *innd* loads *hosts.nntp* and *newsfeeds* into memory during processing, so the server must be "reloaded" after they are edited. *nntpsendctl* and *passwd.nntp* are read each time *nntpsend* is executed (by default, once every ten minutes). It is advisable to do the following:

- a) Determine the changes to be made before beginning editing.
- b) Throttle the server while the changes are being made.
- c) Unthrottle the server when done.

The manual (man) pages that cover these operations are:

```
ctlinnd (8)
hosts.nntp (5)
newsfeeds (5)
nntpsendctl (5)
passwd.nntp (5)
innd (8).
```

4.3.6 Creating a Newsgroup.

Creating a Newsgroup on the GCCS News Network is a two-stage process: establishing the Newsgroup on the Network and creating the Newsgroup on each server.

4.3.6.1 Establishing a Newsgroup Across the GCCS Network. Execute the Make Group Segment. This segment allows users to create a newsgroup. It enforces the naming convention specified in the TLCF CONOPS. This

program provides a command-line interface to newsgroup creation.

On all client machines where users who might want to create a newsgroup sit:

Multiple executables in the progs directory work together to provide newsgroup creation. MakeGroup.init is the script called when the "Make Grp" icon is pressed. It creates an xterm and runs MakeGroup inside of it. MakeGroup, in turn, executes news.aut and GetActive to download a list of currently-existing newsgroups. It then prompts the user to get the new newsgroup name, ensures its correctness, and then calls makegroup. Makegroup builds a control message and then calls postnews to post the article to the news server. Note that makegroup runs sgid, and postnews can only be run by root or under group mail. Postnews provides no error checking as far as contents of the article being posted is concerned.

Step 1: Verify installation of required segments:
GCCS COE 2.0.

Step 2: Install News Make Group 1.0.0.2.

The following will be presented to the installer:

Please enter the names of the machines running news servers for this site. This list will be made available as a menu to users running the news client.

Enter the first server name: (server name)

Is <server name> correct? (y/n) [y]:

Please be patient while we ping (server name).

(server name) is alive

Ping confirms that the machine is there.

Entering (server name) into the menu of news servers.

Enter the second server name: (server name).

Allow users to create "*.limited.*" newsgroups. Does this by stripping ".limited.*" off of the newsgroup name -- the control msg will follow the distribution specified by the portion of the newsgroup name which comes before the "limited".

4.3.7 Adding, Deleting, and Modifying Users' Access to News. The file that configures the News server for user authentication is *nnrp.access*. Ignoring comments and blank lines, this file consists of a series of records, one per line. Each record enables access for a machine or a user. The records consist of five fields separated by

colons:

machine:permissions:username:password:newsgroup list.

For GCCS access permissions, no record will contain both a machine name and a user name/password. Our recommendation is to provide only one record in the *nnrp.access* file that does contain a machine specification. It should look as follows:

***:R::!* ,news.announce.default**

This line allows any machine to connect to the News server without user authentication, but only provides read access (no posting), and only provides access to one newsgroup, *news.announce.default*.

Access for individual users is provided by lines which look as follows:

:R P:username:password:!*,group1,group2,group3,...

If the user provides user name and password, this line allows read and post access to the listed newsgroups (*group1*, *group2*, *group3*, etc.). For a user to have any access to a News server (beyond reading the article in *news.announce.default*), that user must have an entry in *nnrp.access*. There is currently no mechanism for a user to modify his or her password; either the user must tell the News administrator what password to enter into *nnrp.access* or, more likely, the administrator will inform the user what their password is.

For a user to be given access to a specific newsgroup, the name of the group must be included in the list of newsgroups in the user's *nnrp.access* record. To remove access, the name need only be removed from the list. Since *nnrp.access* is consulted each time a user connects to the server, there is no need to re-load the server's configuration after editing *nnrp.access*. Note that the list of newsgroups begins with "!*"; the newsreader server understands wildcards, and "!" means "deny access to all newsgroups." If one reads the commas as "except", then "!* ,group1" means "deny access to all newsgroups except group1." Wildcards can also be used to reduce the size of *nnrp.access* records. For example, if the newsgroups *fruit.orange*, *fruit.banana*, *fruit.grape*, *fruit.lemon*, *fruit.lime*, and *fruit.juice* exist on a site's system, and the site wants user *jdoe* to have access to all of them except *fruit.orange*, then the following line can be placed into *nnrp.access*:

:R P:jdoe:passwd:!*,fruit.*,!fruit.orange

This is useful if there will be a number of newsgroups that will be available to all users. Give those newsgroups the same postfix, and give no restricted newsgroups the same postfix -- for example, all unrestricted newsgroups' names will end with ".all". Then, every user's *nnrp.access* line would look like:


```
:R P:jdoe:passwd:!*,*.all,group1,group2
```

This gives access to all newsgroups whose names end in ".all" plus *group1* and *group2*.

The manual (man) pages that cover these operations are:

```
nnrp.access (5)  
nnrpd (8)  
innd (8).
```

4.3.8 How to Support Multiple Newsgroup Access List Maintainers. It may be desirable to delegate responsibility for maintaining the newsgroup access lists. If this is the case, one possibility is to create a new UNIX group (perhaps named *news_access*). Include user *news* in that group, and change the group of the *nnrp.access* file (*chgrp news_access /h/COTS/NEWSS/lib/nnrp.access*) and change the mode of the file to be group-writable (*chmod g+w /h/COTS/NEWSS/lib/nnrp.access*). Now any user included in the group *news_access* can edit the *nnrp.access* file.

A problem with the above approach is that it is impossible to track which users have modified *nnrp.access*. One way to deal with this is to create a new user on the system (*news_access*) with no shell, and make *news* and *news_access* the only two users in group *news_access*. The users who are maintaining newsgroup access lists are given the password to the *news_access* account, and must *su* to that account to edit *nnrp.access* (since *news_access* has no shell, nobody can log in as *news_access*). By forcing users to *su* to *news_access* before editing *nnrp.access*, a record of who has edited *nnrp.access*, and when, is kept in */usr/adm/sulog*.

The manual (man) pages that cover these operations are:

```
chgrp (1)  
group (4)  
su (1).
```

4.3.9 How to Remove a Newsgroup. Removing a newsgroup will be illustrated with the example of removing "group1" from all news servers in the GCCS News network. To direct News administrators on all machines to remove a newsgroup, a control message must be transmitted. To do this, execute the following:

```
makegroup -d any group1
```

Do not enter any text for the one-line description; for the description ending with end of file (EOF), enter an explanation for why the newsgroup is to be removed. Then, when asked "Send, abort or edit?" select "edit." Within the editor, change every occurrence of "newgroup" to "rmgroup." Save the file and quit the editor, and then select "send."

Each News administrator will receive an e-mail message directing him or her to execute the following command:

```
/h/COTS/NEWSS/progs/newsbin/ctlinnd rmggroup group1
```

Executing this command will remove the newsgroup from the server. The newsgroups file should be edited to remove mention of the newsgroup from it, *nnrp.access* should be edited to remove references to group1, and, if the newsgroup was moderated, moderators should be edited to remove the group1 entry.

The manual (man) pages that cover these operations are:
ctlinnd (8).

4.3.10 Archiving a Newsgroup

4.3.10.1 Why Archive a Newsgroup? Before discussing how to archive a newsgroup, we will discuss why one might that to archive a newsgroup. In addition to holding every "current" news article on disk, the news server maintains a database that tracks the current articles. An article remains current until it expires, at which point the article is removed from the spool and reference to it is removed from the history database (eventually).

The length of time an article remains current is controlled by a combination of the "Expires: " header in the article (if one exists) and the file *expire.ctl* in */h/COTS/NEWSS/lib*. Establishing values for *expire.ctl* will involve a tradeoff between restricting the number of current articles and giving users time to read articles before they are purged from the system.

Under certain circumstances it will be desirable for articles in a particular newsgroup to remain available indefinitely. For example, *news.announce.newusers* is a newsgroup that contains a single article, which should always be on the system. This is accomplished in *expire.ctl*, by specifying "never" for when articles will be purged.

The performance of many of the operations fundamental to News server operation, such as maintaining the history database, searching for articles, etc., depends directly upon the number of current articles. In other words, if the number of current articles is allowed to grow indefinitely, eventually the News server will grind to a halt. Further, the amount of disk space required for the News spool and the history database grows with the number of current articles. Thus, for a newsgroup that receives a steady stream of articles, keeping the articles current forever by default is not an appropriate option.

Another way to keep all of the articles in a newsgroup indefinitely is to archive the newsgroup. The News server has software that allows for the creation of a directory tree, similar to the News spool, in which articles from specified newsgroups are stored. Since these copies of

the articles are not part of the News system (i.e., they are not tracked by the history database, etc.), the size of the archive does not impact the performance of the server.

4.3.10.2 How to Archive a Newsgroup. The program `archive` `/h/COTS/NEWSS/progs/newsbin/archive` can be used to archive a newsgroup. There are two ways to use this program; an archive entry in the `newsfeeds` file can be created, in which case new articles will be archived each time `nntpsend` is executed (every 10 minutes), or archive can be run from a cron entry (presumably before `expire` is run each night).

NOTE: Currently the archive program has undergone only limited development and needs modification. News articles are stored in plain text files in the News spool directory `/h/COTS/NEWSS/spool/news`. The directory hierarchy under the News spool directory matches the newsgroups naming hierarchy. Articles posted to newsgroup `fruit.frozen.blender` will be stored in files in the directory `/h/COTS/NEWSS/spool/news/fruit/frozen/blender`. The names of the files are integers. If a site is dissatisfied with the archiving software, it can mimic the archiver using `crontab` and the UNIX command "find."

The manual (`man`) pages that cover these operations are:
 `crontab` (1)
 `cron` (4)
 `archive` (8).

4.3.10.3 How to Access Archived Articles. There is currently no interface for accessing archived news articles. They will simply be files under `/h/COTS/NEWSS/spool/news/news.archive`.

4.3.10.4 How to Read NEWSS Man Pages. To access the man pages associated with the NEWSS segment, execute the following command:

```
setenv MANPATH ${MANPATH}:/h/COTS/NEWSS/man ; # for csh
set MANPATH=$MANPATH:/h/COTS/NEWSS/man; # for sh, ksh
```

Now, the command `man innd` will access the man page for `innd` (which is in `/h/COTS/NEWSS/man/man8`).

4.3.11 What to Do if Disaster Strikes:

- **Corrupted active file.** The active file is the database of currently active newsgroups. The man page "news-recovery" contains a clear explanation of how to rebuild an active file. If a site wants/needs an old version of the active file to perform the rebuild, and no active file is available, it should be able to ask a neighboring server to send you theirs (this is a good reason

to maintain multiple News servers at a site).

- **Corrupted history file.** The history database can be rebuilt using *makehistory*. See the man pages on *news-recovery* and *makehistory*.
- **Neighboring servers have gone down.** In the GCCS News network topology, each server is provided with multiple neighbors. Thus, the loss of a single neighbor should not prevent a server from receiving News articles except for those newsgroups that are being given a restricted distribution. If a site has a newsgroup that comes to it from only one neighboring server, and that server goes down, the site will have to contact an administrator for that server and find out a) if that server will be back up soon and b) if it won't, the name of a News administrator of a server further upstream that will link to the site's server. Note that if the site can wait until the original neighbor comes back up, it is unlikely to miss articles, but if it has to establish a new connection, articles posted in the interim between the original neighbor going down and the new neighbor being established will not be transmitted to the site's server automatically.
- **News server has gone down.** If the site's News server has gone down, but will be back up within an hour or two, then, when the site's server is back up, the neighboring servers will transmit the news articles they have accumulated in the interim. If the server will be down for an extended period of time, it is important to notify the users and provide them an alternate server to which they can connect. Further, the site must provide the neighboring servers with a machine to which to transmit news articles. An option is for the administrator to have given the site's news server an alias. For example, if the News server is at FORSCOM and is running on [gidget.forscom.gcc.smil], create a DNS alias [news.forscom.gcc.smil], and give that as the name of the news server to users and neighboring servers. Then, if [gidget] goes down in a permanent way, the site can install the NEWSS segment on a new machine, restore the most recent copies of the configuration files (*active*, *newsfeeds*, etc.), restore as much of the spool as can be recovered (the site may wish to ftp portions of the spool from neighboring sites to ensure that no articles are lost) and then change the [news.forscom.gcc.smil] alias to point to the new News server.
- **Lost spool (lost all articles).** First, the server must be throttled. Second, a News disk partition must be allocated for use as a News spool. Once a new partition is assigned to be the News spool (mounted on /h/s3, for example), a parent directory for the News spool must be created in that partition /h/s3/*spool.news* and the symbolic link /h/COTS/NEWSS/*spool* must be set to point to it (*rm /h/COTS/NEWSS/spool; ln -s /h/s3/spool.news /h/COTS/NEWSS/spool*). Then, a neighboring server (hopefully one at the same site) can provide a copy of their spool to be ftp'ed

into the spool partition. Finally, the active file and history database can be rebuilt, and the News server unthrottled (allowing neighbors to resume feeding News articles to this server).

The manual (man) pages that cover these operations are:

- ctlinnd (8)
- news-recovery (8)
- innd (8).

4.3.12 News Make Group

This segment allows users to create a newsgroup. It enforces the naming convention specified in the TLCF CONOPS. This program provides a command-line interface to newsgroup creation.

On all client machines where users who might want to create a newsgroup sit:

Multiple executables in the progs directory work together to provide newsgroup creation. MakeGroup.init is the script called when the "Make Grp" icon is pressed. It creates an xterm and runs MakeGroup inside of it. MakeGroup, in turn, executes news.aut and GetActive to download a list of currently-existing newsgroups. It then prompts the user to get the new newsgroup name, ensures its correctness, and then calls makegroup. Makegroup builds a control message and then calls postnews to post the article to the news server. Note that makegroup runs sgid, and postnews can only be run by root or under group mail. Postnews provides no error checking as far as contents of the article being posted is concerned.

Step 1: Verify installation of required segments:
GCCS COE 2.0.

Step 2: Install News Make Group 1.0.0.2.

The following will be presented to the installer:

Please enter the names of the machines running news servers for this site. This list will be made available as a menu to users running the news client.

Enter the first server name: (server name)

Is <server name> correct? (y/n) [y]:

Please be patient while we ping (server name).

(server name) is alive

Ping confirms that the machine is there.

Entering (server name) into the menu of news servers.

Enter the second server name: (server name).

Allow users to create "*.limited.*" newsgroups. Does this by stripping ".limited.*" off of the newsgroup name -- the control msg will follow the distribution specified by the portion of the newsgroup name which comes before the "limited".

4.4.1 Netsite Installation. Netsite is the commercial Web server that will be provided to certain GCCS sites. For Netsite, the installer will be asked for the machine name and the domain name. The install script then activates a Web browser, which will ask the installer to establish a name and a password for the Web server administrator.

4.4.2 httpd Installation. The public-domain Web server provided to GCCS is httpd. When the PostInstall file is executed it will ask for the name or IP address of the machine the site is running the installation on. If the site is running the installation from a remote machine, enter the IP address of that machine. This is used to set the display so errors and information will be shown on the active machine. A log is created in *./POSTINSTALL.log*.

The install configures the httpd server, builds a default home page, and sends mail to *smith5m@trudel.osf.gcc.smil* to let them know that a new Web server is up.

The installer will then be asked for the full name of the site's System Administrator so mail can be sent to the SA.

To de-install the segment, run the DE-INSTALL script.

SECTION 5. DOMAIN NAME SERVICE ADMINISTRATION

5.1 Overview

Every network device attached to a TCP/IP network is identified by a unique 32-bit IP address. Any device that has an IP address can be assigned a host name. While host names are not required--they simply make it easier for the user to use the network and may be used interchangeably with a system's IP address.

Currently three popular methods are used to translate or resolve host names into IP addresses in GCCS:

- Host Tables (/etc/hosts)
- NIS+
- Domain Name Service (DNS)

Host tables are located on each system on the network in the *etc* directory. This requires that each table be maintained separately and, typically, can be an administrative burden on all but the smallest of networks.

When using NIS+, a single host file, found under */h/EM/nis_files/host* in the GCCS EM server, is used by all GCCS platforms. It should not be used to resolve names of platforms outside the site's LAN.

DNS is an application layer protocol that is part of the standard TCP/IP protocol suite. DNS is in essence a naming service; it obtains and provides information about hosts on a network.

DNS performs naming between hosts within the local administrative domain and across domain boundaries. It is distributed among a set of servers, commonly known as "name servers," each of which implements DNS by running a daemon called *named*.

5.2 References

- a. *Administering NIS+ and DNS* (Solaris Manual)
- b. *DNS and BIND* (O'Reilly & Associates, Inc, Paul Albitz & Cricket Liu)
- c. DNS template files are loaded onto the designated DNS system in */var/nameser* by the GCCS COE Kernel tape, if the installer requests them.

Template files are also available from the SIPRnet Support Center (SSC) through an "anonymous ftp" account at *ss.smil.mil* (IP address 204.34.130.5)

Instruction for getting DNS Template files via ftp:

```
Host_name > ftp ssc.smil.mil
Connected to ssc.smil.mil
220 ***** Welcome to the SIPRNET Support Center (SSC) *****
***** Login with username "anonymous"
Sipr - SIPRnet Management Information
templates - Registration Template
netinfo - SSC Information Files
rfc - Request for Comments Repository
std - Internet Protocol Standards
220 and more!
Name (ssc.smil.mil.user): anonymous
331 Guest login ok, send your email address as password
Passowrd: xxxxxxxx
230 Guest login ok, access restrictions apply
ftp > cd domain
ftp > mget *
ftp > bye
221 Goodbye
```

If Netscape is implemented on the host system, the SSC can be contacted via Web page "<http://ssc.smil.mil>."

5.3 Pre-Installation Tasks

Before beginning the DNS installation, perform the following tasks:

- a. Choose two reliable UNIX machines on the LAN to be the primary and secondary name servers. Any UNIX device with the *bind* or *in.named* daemon can run the name server software. These local name servers will be set up to know the addresses and aliases of all the local devices and to know where to look for information about devices in other domains. The name server software does not require dedicated machines.

NOTE: All *SIPRNET* domain names end with *disa.smil.mil*

- b. Choose a DNS domain name. Table 5-1 provides a partial list. (Names listed can be verified by calling the Hotline at the DISA OSF.) A DNS domain name is not the same as the NIS or NIS+ domain name. The NIS or NIS+ domain name is what the user gets after entering the command *domainname*. Some examples of fully qualified DNS domain names are:

```
the osf uses:    osf.disa.smil.mil
the jdef uses:   jdef.disa.smil.mil
centcom uses:    cent.smil.mil
```

- c. Register site name servers with the SSC. To notify the SSC

of a new name server, obtain the registration template from the anonymous FTP or HTTP server "ssc.smil.mil", complete the document including fully qualified domain names of the name server hosts, their IP addresses, and a technical point of contact (POC), and email the document to the SSC at **HOSTMASTER@SSC.SMIL.MIL**.

5.4 Installing the Primary Name Server

WARNING: Be very careful of the syntax and location of white space and "." in these files; they must be exact or they will not work and the installer will not receive a clear indication of failure. There are four important, but easily overlooked, syntactical errors that can occur:

- a. There must be a dot at the end of the fully qualified names; e.g.,

hornet.osf.disa.smil.mil.

The final dot lets DNS know to start at the root server.

- b. Make sure there are no uncommented white lines or the file will not be fully read. Comments in these files are noted by a semi-colon (;) at the beginning of each comment line.
 - c. The *db.hosts*, *db.rev.hosts*, and *db.local* files have a serial number in their files. This number needs to be incremented each time these files are edited. If the site does not increment this number, the DNS daemon will not know there has been a change and will not read any edits. This problem will be discovered when the edited file is chosen.
 - d. The *db.cache* file has a "dot" at the beginning of the lines that identify the root name servers. DNS will not function properly without the dots.
-

The following files are located in */var/nameserver*.

NOTE: These are examples and must be modified for the site.

<i>db.hosts</i>	Maps local domain names and aliases to addresses.
<i>db.rev.hosts</i>	Maps addresses to local domain names.
<i>db.cache</i>	Root name server address locations.
<i>db.local</i>	Loopback network.
<i>named.boot</i>	Ties all the other files together.

NOTE: These files are generally referred to as the name server database (*db.xxx*) files and can have any name the site chooses.

- a. Set up the *db.hosts* file. This file, with the *db.rev.hosts* file, defines the domain for which a site's name server is authoritative (the best source of information). It contains the following types of records:

SOA	Start of authority is always the first entry. There can be only one in a database file.
NS	Lists a name server for this domain.
A	Maps a name to an address.
CNAME	Defines an alias (called a canonical name).
PTR	Maps an address to a name.
MX	Mail Exchanger defines a mail hub for the local network.

NOTE: This list is not an exhaustive list of all available record types. It supplies enough to begin setting up the file.

The following is a sample *db.host* file:

NOTE: A semi-colon (;) indicates a comment.

```
;
; Name Server tables for the server at jdef.disa.smil.mil
;
; Last update Wed Mar 10 20:16:33 1993
;
@ IN SOA  backfire.jdef.disa.smil.mil.
root.backfire.jdef.disa.smil.mil. (
    93051013      ; serial number
    3600          ; refresh after 1 hour
    300           ; retry after 5 minutes
    604800        ; expire after 1 week
    3600          ; minimum time to live (ttl) of 1
                  ; hour
jdef.disa.smil.mil. IN NS  backfire.jdef.disa.smil.mil.
                   IN NS  jdef1000.jdef.disa.smil.mil.
                   $ORIGIN jdef.disa.smil.mil.
backfire  IN A      199.114.66.86
mailhost  IN CNAME  backfire.jdef.disa.smil.mil.
jdefrouter IN A      199.114.66.90
jdef1000  IN A      199.114.66.80
GCCS_SRV  IN CNAME  jdef1000.jdef.disa.smil.mil.
UCCS_SRV  IN CNAME  jdef1000.jdef.disa.smil.mil.
uccs_server IN CNAME jdef1000.jdef.disa.smil.mil.
gsorts    IN CNAME  backfire.jdef.disa.smil.mil.
jws3      IN A      199.114.66.70
jots1     IN A      199.114.66.89
localhost IN A      127.0.0.1
;
```

NOTE: The dot (".") at the end of a fully qualified name means to start at the root domain.

When a record is changed in a database file, the corresponding serial number should always be incremented. Having made this change, the name server daemon can then be signaled to check the database and update its records and the secondary name server's records. A good practice is to use the date and time the serial the number in *YYMMDDHH* format.

The *root.jdef.disa.smil.mil.* is the mail address for the person responsible for this domain.

- b. Set up the *db.rev.hosts* file. Because addresses are looked up as names in DNS, addresses must also be provided to name mappings. Each host in the domain must have at least one record. The addresses are reversed with *in-addr.arpa* appended. The following is an example of the *db.rev.hosts* file:

```
;
; Last update Fri Jun 24 10:40:23 1994
;
@   IN SOA   backfire.jdef.disa.smil.mil.
      root.backfire.jdef.disa.smil.mil.
      93051013      ; serial number
      3600          ; refresh after 1 hour
      300           ; retry after 5 minutes
      604800        ; expire after 1 week
      3600          ; minimum time to live
                        ;(ttl) of 1 hour

      IN NS       backfire.jdef.disa.smil.mil.
      IN NS       jdef1000.jdef.disa.smil.mil.
      $ORIGIN 66.114.199.in-addr.arpa.
86   IN PTR       backfire.jdef.disa.smil.mil.
80   IN PTR       jdef1000.jdef.disa.smil.mil.
90   IN PTR       jdefrouter.jdef.disa.smil.mil.
70   IN PTR       jws3.jdef.disa.smil.mil.
89   IN PTR       jots1.jdef.disa.smil.mil.
;
```

- c. Set up the *db.cache* file. The name server daemon uses the cache information to resolve an address outside its local domain. The cache points to the primary and secondary root name servers, *hornet.osf.disa.smil.mil* and *milo.osf.disa.smil.mil*, respectively. These name servers are located at the OSF and are aware of all the other name servers in the network. An alternate root name server is needed to protect against an OSF site failure. Sites that would like to volunteer to provide this service should mail

to "netadm@osf.disa.smil.mil". The *db.cache* file should look exactly like the following:

```

          3600000 IN      NS      ROOT1.SSC.SMIL.MIL.
ROOT1.SSC.SMIL.MIL. 3600000 A      204.34.130.4
          3600000 NS      ROOT2.SSC.SMIL.MIL.
ROOT2.SSC.SMIL.MIL. 3600000 A      140.49.179.234
          3600000 NS      ROOT3.SSC.SMIL.MIL.
ROOT3.SSC.SMIL.MIL. 3600000 A      140.49.183.234
          3600000 NS      ROOT4.SSC.SMIL.MIL.
ROOT4.SSC.SMIL.MIL. 3600000 A      199.252.79.234

```

When an alternate root name server is defined, it will be added here.

- d. Set up the *db.local* file. This file provides the loopback address. The following is an example of this file:

```

;
; name.local for jdef
;
$ORIGIN jdef.disa.smil.mil.
@ IN SOA  backfire.jdef.disa.smil.mil.
root.backfire.jdef.disa.smil.mil.(93051013
                                ; serial number
                                3600      ; refresh after 1 hour
                                300       ; retry after 5 minutes
                                604800    ; expire after 1 week
                                3600 )    ; minimum time to live (ttl)
                                of 1 hour
;
  IN      NS      backfire.jdef.disa.smil.mil.
  IN      NS      jdef1000.jdef.disa.smil.mil.
;  IN      PTR      localhost.
;
; So much for wraparound 127.0.0.1
;

```

- e. Set up the *named.boot* file. This file ties all of the database files together. It specifies the catalog where the database files reside, and the file name the site has chosen for each database. The following is an example of the *named.boot* file:

```

;
; named.boot for primary name server for your domain
;
;type          domain          sourcefile or host
;
directory  /var/nameserver
cache      .
db.cache
primary    jdef.disa.smil.mil    db.hosts
primary    66.114.199.in-addr.arpa db.rev.hosts

```

```
primary          0.0.127.in-addr.arpa      db.local
;
```

When all the database files and the *named.boot* file are completed, copy the *named.boot* file to */etc/named.boot* directory:

```
# cp /var/nameserver/named.boot /etc/named.boot<return>
```

To start the name server daemon, as **root** enter:

```
# in.named<return>
```

During system startup, if the */etc/named.boot* file exists, the *in.named* daemon will be automatically started.

- f. Set up the */etc/resolv.conf* file. This file defines the name servers for a domain. Set it up as follows:

```
domain yourdomain.disa.smil.mil<return>
nameserver ip_address_of_primary_name_server<return>
nameserver ip_address_of_secondary_name_server<return>
nameserver ip_address_of_offsite_backup_name_server<return>
```

Be sure there are no extra lines or spaces at the end of a line. If there are extra spaces, the resolver does not work, and it does not provide any error messages. For devices in a domain that are not name servers, this is the pathway to a name server. A maximum of three name servers may be listed in the resolver.

- g. Perform the following steps to complete the installation:

1. Verify that the */etc/defaultrouter* file contains the IP address for the site's gateway. If this file does not exist, or contains the wrong value, create it and add the IP address of the default gateway.

2. To dynamically set the default gateway, type:

```
# route add net default <IP_address> 1<return>
```

3. Verify the netmasks using the "ifconfig" command:

```
# ifconfig le0<return>
```

The following is an example of a Class B network with a Class C netmask:

```
le0 : flags = 863<up , broadcast , notrailers , running , multicast > mtu 1500
      inet 164.117.210.77 netmask . fffffff0 broadcast 164.117.210.255
```

NOTE: 164.117.210.77 should be your host's IP address.

("Netmask" should be ffff0000 if Class B netmask is desired. It should match A.2.

"Broadcast" should be 164.117.255.255 if Class B network is desired.)

4. To update a non-NIS system, edit */etc/netmasks* and enter the command:

```
# ifconfig -a netmask + broadcast +<return>
```

5.5 Secondary Name Server Setup

- a. Create a catalog like */var/nameserver* like the primary name server. Touch the *db.hosts* and *db.rev.hosts* files as follows:

```
# mkdir /var/nameserver<return>
# cd /var/nameserver<return>
# touch db.hosts db.rev.hosts<return>
```

- b. Create or copy the *named.boot*, *db.cache*, and *db.local* files from the primary server. In the *named.boot* file, change every occurrence of primary to secondary except for the *db.local* entry. For the *db.hosts* and *db.rev.hosts* files, add the IP address of the primary server. The file should be similar to the following:

```
;
; Secondary (backup) nameserver
;
;type      domain    sourcefile or ip address
;
directory  /var/nameserver
cache      .
db.cache
secondary  jdef.disa.smil.mil      199.114.66.86 db.hosts
secondary  66.114.199.in-addr.arpa 199.114.66.86 db.rev.hosts
primary    0.0.127.in-addr.arpa    db.local
;
```

Copy the file to */etc/named.boot* and start the name server daemon.

5.6 Set Up the Remaining Hosts on the Network

The remaining hosts use the */etc/resolv.conf* file to locate the name servers for a domain. Set up the remaining hosts as follows:

```
domain {your domain}.disa.smil.mil
nameserver {ip_address_of_primary_name_server}
nameserver {ip_address_of_secondary_name_server}
nameserver {ip_address_of_offsite_backup_name_server}
```

Be sure there are no extra lines or spaces at the end of a line. If there are extra spaces, the resolver does not work, and it does not provide any error messages. A maximum of three name servers may be listed in the resolver.

5.7 Debugging Hints

- If the *in.named* daemon does not start:

First check the */var/adm/messages* file. An error message is printed there if *syslog* is turned on.

- If things are not working as expected:

Check the cache by signaling the *in.named* daemon as follows:

```
# kill -INT `cat /etc/named.pid`<return>
```

This will cause a dump to the */var/tmp/named_dump.db* file.

- The *nslookup* facility provides insight into how DNS sees the network. Enter the command **nslookup** and use *help* to get a list of available options.

5.8 Updating the Name Server Database

Edit the files as appropriate, making sure to increment the serial number (always edit the files on the primary). Signal the *in.named* daemon of the change, using the following command. This command will insert the process ID (pid) of the named daemon as an argument for the kill command (HUP is the UNIX signal name for Hangup):

```
kill -HUP `cat /etc/named.pid`<return>
```

Force an update of the secondary name server using the following command:

```
usr/sbin/in.named -xfer -z jdef.disa.smil.mil -f db.hosts -s 0
backfire.jdef.disa.smil.mil <return>
```

NOTE: Substitute site-specific information for "backfire.jdef".

z = the zone
f = the database to update
s = the serial number on the secondary server is the same as the

on the primary server.

If the above command does not work, do the following on the secondary name server: kill the *in.named* daemon, remove the *db.hosts* and *db.rev.hosts* from the secondary, touch the *db.hosts* and *db.rev.hosts* files, then restart the daemon. These actions force an update.

5.9 Solaris 2.3 Specifics

Make sure the */etc/nsswitch.conf* file reflects DNS resolution. Typically the host map should be like the following:

```
files dns nisplus [NOTFOUND=return]    if running nis+
files dns [NOTFOUND=return]            if not running nis+
```

NOTE: "files" has been placed first for those sites that have "hot standby" ORACLE database servers. If the primary database server goes down, the site only has to update the */etc/inet/hosts* file to activate the backup.

SECTION 6. NIS+ ADMINISTRATION

6.1 Overview of NIS+

NIS+ stands for Network Information Service Plus. It was designed to replace NIS, and is a default naming service for Solaris. NIS+ can provide limited support to NIS clients via a YP-compatibility mode. NIS+ was mainly designed to address problems that NIS cannot address.

It is important to note that there is no relation between NIS+ and NIS. The commands and the overall structure of NIS+ are different from NIS. In addition, some command syntax in NIS+ is different from the NIS commands. NIS+ was designed from scratch.

NIS+ increases security by using an additional authentication method. Users will still have their standard log-in password, will give them access to the system. They will also have a secure rpc password or network password. This new password is necessary to actually access NIS+, and is what provides the new security. Usually, a user's login password and network password will be the same, and a user will automatically have access to all NIS+ functionality when they log in with their log-in password. However, if they are different, a user will have to *keylogin* and type his or her network password to get access to NIS+. Special notes are the NIS+ daemons *rpc.nisd* and *nisd_cachemgr*. You should see them running on every NIS+ server and client.

6.1.1 An Explanation of the Basic NIS+ Objects. NIS+ objects are structural elements used to build and define the NIS+ namespace. The five basic NIS+ objects are described in the subsections that follow. Objects are always separated by dots.

6.1.1.1 Directory Objects. These are similar to Unix system directories, in that they can contain one or more objects such as: table objects, group objects, entry objects, or link objects. Directory objects form an inverted tree-like structure, with the root domain at the top and the subdomains branching downwards. They are used to divide namespace into the different parts. Each main directory object will contain that domain's *org_dir* and *groups_dir* directory objects. The *org_dir* directory objects contain table objects for that domain. The *groups_dir* directory objects contain NIS+ administrative group objects.

Example of Directory Objects:

```
Sun.Com.  
org_dir.Sun.Com.  
groups_dir.Sun.Com.
```

6.1.1.2 Table Objects. These are similar to NIS maps. Table objects store a variety of network information. Tables may contain zero or more Entry Objects. There are a total of 17 predefined table objects.

Tables can be administered with the *nistbladm* or *nisaddent* commands. Table entry objects form a row in the table and each row stores one record.

Example of Table Objects:

Passwd.org_dir.Sun.Com.
Hosts.org_dir.Sun.Com.

Example of Entry Objects:

[name=user1],passwd.org_dir.Sun.Com.

6.1.1.3 Group Objects. These are NIS+ namespace administrative user groups. They permit controlled access rights to namespace modification on a group basis. They are administered with the *nisgrpadm* command.

Example of Group Objects:

admin.groups_dir.Sun.Com.

6.1.1.4 Link Objects. These are pointers to other objects. They are similar to symbolic links. They typically point to table or object entries. They are administered with the *nisln* command.

6.2 Debugging NIS+. Before trying to debug a NIS+ problem, you should always make sure that you have the recommended patches installed on the system. In particular, the kernel patch should be at the current patch level, and all the systems should have the same patch revision.

6.2.1 Authentication Problems. Most of the problems in NIS+ are authentication-related problems. Assuming that you are running *rpc.nisd* at security level 2 on your master server, you can use *niscat* to determine if a user is authenticated:

```
% niscat passwd.org_dir
```

If the user can see the encrypted passwords, then the user is authenticated. If the user sees *NP* in place of encrypted passwords, then the user does not have permission to read the "passwd" column. In this case, you could run *keylogin* to try and reauthenticate the user. If that works, the user might need to run *chkey* to synchronize the login and network passwords.

If *keylogin* still does not authenticate the user, it is likely that the user's credentials have not been set up correctly. You can check that someone actually has credentials by examining the *cred* table:

```
% niscat cred.org_dir
```

You can create credentials for a user with *nisclient*:

```
% nisclient -c username
```

When having credential problems, also consider that it might be a problem with the credentials of the workstation as well. If known-good users fail on a specific workstation, you will probably want to try and set the workstation back up, as described in Section 6.3.3.

6.2.2 Examining NIS+ Tables. Some NIS+ problems will be related to information missing from tables. You can examine the contents of tables with a variety of commands:

niscat will output the entire contents of a table for you:

```
% niscat passwd.org_dir
```

You can also examine the object properties of a table:

```
% niscat -o passwd.org_dir
```

This can be very helpful, because it will show you if a table has unusual permissions which may be restricting access.

nismatch can also be used to find things in a table:

```
% nismatch -h joe passwd.org_dir
```

niscat and *nismatch* both directly access the NIS+ tables. *getent*, on the other hand, will look up tables in the order defined in the */etc/nsswitch.conf*. A typical *getent* command would be the following:

```
% getent passwd joe
```

This would look up the user *joe* in *passwd*. In a typical environment, it would access files first, and then NIS+. If you find that *getent* and *nismatch* give you different answers, you should look at your *nsswitch.conf*. Perhaps a naming service that is listed earlier in your *nsswitch.conf* has different information, or NIS+ may not be listed at all in your *nsswitch.conf*.

6.2.3 Using Snoop. If you are having intermittent problems, *snoop* is often useful to debug them. To use *snoop* correctly, you must run it from an uninvolved machine. For example, if you have a client that is having intermittent problems with NIS+, you should run *snoop* on a machine on the same subnet as the problem client, but the machine must be neither the client nor any of the NIS+ servers:

```
unrelated-machine# snoop problem-machine
```

This will tell you about all of the packets going in and out of the problem machine. You should look for NIS+ packets, taking careful notes of errors. If you are getting some type of intermittent errors, it is useful to see which server your client was talking with at the time of your problem. Possibly one of your servers has bad or old information.

6.2.4 Performance Problems. Some NIS+ problems may be related to performance. You might find NIS+ servers overloaded. You might get "NIS+ Server Unreachable" errors because your network is overloaded. The commands *snoop* and *netstat* may be used to examine such problems further. Sections 6.5 and 6.9 explain other places you can get help from within Sun. Performance Tuning is beyond the scope of the help that SunService can provide.

6.2.5 GCCS Version 2.2 Information. In GCCS Version 2.2 the ASCII versions of the NIS+ tables are stored in */etc/nis*. The System Maintenance segment will update those tables daily, except for the shadow file, which is updated every hour. When performing a "NIS populate" */etc/nis* should be specified as the location of the NIS+ tables.

Several scripts are located in */etc/nis/admin* to assist the system administrator. The script "nis_kill" kills all NIS+ processes and restores the system files to reflect a non-NIS+ system. The "nis_client" makes a system a NIS+ client when executed. The "nis_server" and "nis_server_post" scripts make a system a NIS+ server and populate the NIS+ tables. The NIS+ domain name and the NIS+ server name that are found in the "nis_client" and "nis_server" scripts is updated, if necessary, the System Maintenance segment on a daily basis.

6.3 Common How-Tos

6.3.1 How to Prepare Your Site for NIS+. Before configuring the NIS+ namespace you need to do initial planning, including: verifying hardware and software requirements, naming the domain, determining security level, and planning your domain hierarchy.

In general you need a Solaris 2.3 or higher operating system: 32 to 64 MB of memory and about 128 MB of swap space is recommended for a medium to large domain. The size of */var/nis* is recommended to be about 20 MB. All of these requirements can be found in Section 7.4 of the *Administering Name Services Manual*.

The domain name for the root server should be at least two labels long. This means for example, that the domain name "xyz." is not supported, but the domain name "xyz.com." is.

Another consideration is security level. The default security level is 2. If you want a secure environment, then you should run NIS+ at security level 2. If you have SunOS client machines on the network, which are going to get served by the NIS+ server, then you need to run

NIS+ in YP compatibility mode. You should also decide about the access rights you want to give to users and administrative groups.

Finally, you should understand NIS+ concepts such as the difference between the log-in password and the network password. It's very important to know this difference while troubleshooting authentication-related problems.

Once you are ready to begin configuring your domain, it is recommended that you use the quick startup scripts to configure NIS+ namespace. For example, to configure the root server use the *nissserver* script; to configure clients use the *nisclient* script. These scripts are easy to use and reduce chances for errors. The following Sections outline the use of these scripts.

6.3.2 How to Set Up a Root NIS+ Master. To set up a root server, become the superuser on the root master, and use the *nissserver* script to build the root domain:

```
root-server# nissserver -v -r -d domain_name
```

(where domain_name is your NIS+ domain.)

Afterward, you will want to populate the NIS+ tables from a set of ASCII files. It is a good idea to create a separate directory and then edit the files required to populate the tables there.

For example, create a directory */var/tmp/nisfiles* and copy the files from the */etc* directory to */var/tmp/nisfiles*, and then edit the files. You may wish to edit the *passwd* file, for example, because you only need the entries for the normal users in the NIS+ *passwd* table.

Following is the list of standard NIS+ tables that you may wish to include when you populate your maps (although it is not required that they all be included):

```
aliases
auto_home
auto_master
bootparams
cred
group
hosts
netgroups
netmasks
networks
passwd
protocols
rpc
services
timezone
```

To populate the tables, change to the directory where the edited files are, and then run the *nispopulate* script:

```
root-master# cd /var/tmp/nisfiles
root-master# nispopulate -v -F
```

It is important to note that the network password created in the credential table for all the users is "nisplus". This should be changed to something more secure. For normal users, every user needs to run *keylogin* and then do the *chkey* command, and enter a new network password. It is highly recommended that login password and the network password be the same. In the NIS+ environment, *login* explicitly runs *keylogin* so if the network password is same as the log-in password, users don't have to do a separate *keylogin* to authenticate.

When the *nispopulate* is done, you should reboot your server. When it comes back up, you can verify that NIS+ is working correctly by running the standard NIS+ commands:

```
root-master% nisl
root-master% niscat passwd.org_dir
```

6.3.3 How to Set Up a NIS+ Client. To set up a NIS+ client, first become **root** on the master server, and verify that NIS+ host table has an entry for the client. If it does not, use *admintool* to add it. Afterward, run the *nisclient* script to create credentials for the client machine:

```
root-master# nisclient -v -d domain_name -c client_machine
```

(where *domain_name* is your NIS+ domain, and *client_machine* is the name of your new client.)

Do not worry if *nisclient* tells you that the credentials already exist for your *client_machine*.

Next, log in to your client machine as **root**, and run *nisclient* to initialize it:

```
client# nisclient -v -i -h master_machine -a master_ip -d
domain_name
```

(where *master_machine* is the name of your NIS+ master, *master_ip* is the IP address of your NIS+ master and *domain_name* is the name of your NIS+ domain.)

6.3.4 How to Set Up a Root NIS+ Replica.

After your root replica has been set up as a client system (see Section

6.3.3), start the NIS+ server daemon:

```
root-replica# rpc.nisd
```

Then, you can execute the *nissserver* command on the root-master:

```
root-master# nissserver -v -R -d domain_name -h replica_machine
```

(where *domain_name* is your NIS+ domain and *replica_machine* is the name of your root-replica.)

Finally, run *nisping* on the master server to propagate the tables to the replica server:

```
root-master# nisping domain_name.  
root-master# nisping org_dir.domain_name.  
root-master# nisping groups_dir.domain_name.
```

(where *domain_name* is your NIS+ domain.)

6.3.5 How to Set Up a Subdomain NIS+ Master. The subdomain server must already be setup as a client of the domain above it (see Section 6.3.3). This may be the root domain, or some subdomain. After it is, you should start *rpc.nisd*:

```
subdomain-master# rpc.nisd
```

Then, you should log in to the master of the domain above your current domain, and execute *nissserver* (*root-master* is used in this example, but this could also be some higher subdomain-master):

```
root-master# nissserver -v -M -d subdomain_name -h subdomain_master
```

(where *subdomain_name* is the name of your new NIS+ subdomain, and *subdomain_master* is the name of your Subdomain master.)

You will then want to populate the NIS+ tables for your new subdomain. This is done on your subdomain master, in a similar manner to that described in Section 6.3.2:

```
subdomain-master# cd /var/tmp/nisfiles  
subdomain-master# nispopulate -v -F
```

Afterward, reboot your new subdomain master.

6.3.6 How to Set Up a Subdomain NIS+ Replica. The same procedure as is described in Section 6.3.4, should be used to set up a Subdomain Replica. However, the commands will be run on the subdomain-master, not the root-master.

6.3.7 How to Configure the Root Server for an IP Address Change.

Unfortunately, there is no easy way to configure the root server again when the IP address is changed. This is because the clients maintain the server's IP address in their cold start file, and the server has the old IP address in its cache. You must totally reinitialize the root server for an IP address change.

The best way to do this is first dump the NIS+ tables to ASCII files using the *nisaddent* command:

```
root-master# cd /var/tmp/nisfiles
root-master# nisaddent -d aliases > aliases
root-master# nisaddent -d bootparams > bootparams
root-master# nisaddent -d ethers > ethers
root-master# nisaddent -d group > group
root-master# nisaddent -d hosts > hosts
root-master# nisaddent -d netgroup > netgroup
root-master# nisaddent -d netid >
root-master# nisaddent -d netmasks > netmasks
root-master# nisaddent -d networks > networks
root-master# nisaddent -d passwd > passwd
root-master# nisaddent -d protocols > protocols
root-master# nisaddent -d publickey > publickey
root-master# nisaddent -d rpc > rpc
root-master# nisaddent -d services > services
root-master# nisaddent -d shadow > shadow
root-master# nisaddent -d timezone > timezone
root-master# nisaddent -d -t auto_home.org_dir key-value >
auto_home
root-master# nisaddent -d -t auto_master.org_dir key-value >
auto_master
```

Then, you must clean out old NIS+ info:

```
root-master# cp /etc/nsswitch.files /etc/nsswitch.conf
root-master# /etc/init.d/rpc stop
root-master# rm -f /etc/.rootkey
root-master# rm -rf /var/nis/*
root-master# /etc/init.d/rpc start
```

And finally, you can reconfigure your NIS+ server, as described in Section 6.3.2.

6.3.8 How to Add a User to the Admin Group. In your default setup, only root on your master machine will be able to make modifications to most of your NIS+ maps. You will probably want to extend these permissions to all of the system administrators. This is typically done by putting all of the system administrators into the admin group:


```
# nisgrpadm -a admin.domain_name. joe  
# nisgrpadm -a admin.domain_name. liz
```

The above command will give "joe" and "liz" the ability to modify most NIS+ tables from their own accounts. This can give considerable privilege, so you should make sure that joe and liz are trusted, and that their accounts are secure.

6.3.9 How to Change a NIS+ User Password.

The password for a normal user can be changed by the user running the *nispasswd* command:

```
% nispasswd
```

This updates the password in the *password* table, and also updates the credential table.

Root can change passwords for users by running:

```
# nispasswd user_name
```

However, this procedure should never be used for changing the root password.

6.3.10 How to Change a NIS+ root password. To change a root passwd, you must use the following procedure.

First, issue the *passwd* command, and supply new password:

```
# passwd
```

This will change the password in the local */etc/passwd* file. Then, run *chkey -p* and enter the new network passwd:

```
# chkey -p
```

Finally, do *keylogin -r* to update */etc/.rootkey* file with the new private key for the server:

```
# keylogin -r
```

This changes the private key for the server, while the public key remains the same. This is necessary because clients use server's public key for authentication.

If you use any other method for updating your root password, you can create serious problems in your NIS+ domain.

6.3.11 How to Administer NIS+ Credentials.

The *nisaddcred* command can be used to create, update and remove local and DES credentials.

To create or update credentials for another NIS+ principal:

```
% nisaddcred -p uid -P principal-name local
% nisaddcred -p rpc-netname -P principal-name des
```

The *rpc-netname* is *unix.uid@domain_name* for a user, and *unix.hostname@domain_name* for the root user on a host. Note that these domainnames do NOT contain a trailing dot, unlike most NIS+ commands. The *principal-name* is *name.domain_name.*, where *name* can be user name or a host name.

For example, joe (uid 555) in the *example.com* domain has the following names:

```
principal-name:    joe.example.com.
rpc-netname:       unix.555@example.com
```

While root on the machine *test* has the following names:

```
principal-name:    test.example.com.
rpc-netname:       unix.test@example.com
```

A few caveats: you can only create DES credentials for a client workstation. DES credentials may only be created in the client's home domain. However, you can create local credentials for a client user in other domains.

To remove credentials execute the following:

```
% nisaddcred -r principal-name
```

6.3.12 How to Administer NIS+ Groups.

The following commands may all be used to administer NIS+ groups. Be aware that NIS+ groups are not the same thing as normal Unix groups.

You can list the object properties of a group with *niscat*:

```
% niscat -o group-name.groups_dir.domain_name.
```

The *nisgrpadm* command creates, deletes, and performs miscellaneous administration operations on the NIS+ groups.

To create a group:

```
% nisgrpadm -c group-name.domain_name.
```

The group you create will inherit all the object properties specified in the NIS_DEFAULTS variable. You can view the defaults using the *nisdefaults* command:

```
root-master# nisdefaults
principal name: master.domain_name
domain name: domain_name
Host Name: master.domain_name
Group Name:
Access Rights: ----rmcdr---r---
Time to live: 12:0:0
Search Patch: domain-name
```

To delete a group:

```
% nisgrpadm -d group-name.domain_name.
```

To list the group members:

```
% nisgrpadm -l group-name.domain_name.
```

To add members to a NIS+ group:

```
% nisgrpadm -a group-name member
```

To remove members from a NIS+ group:

```
% nisgrpadm -r group-name member
```

To determine if a member belongs to a NIS+ group:

```
% nisgrpadm -t group-name member
```

6.3.13 How to Administer NIS+ Tables.

The *nistbladm* command is the primary NIS+ table administration utility. With this command, you can create, modify, or delete tables and table entries. To create a table you must have create rights to the directory under which you will create. To delete a table you must have destroy rights to the directory. To modify a table, or to add, change, or delete the entries you must have modify rights to the table or the entries.

A table column can have following characteristics:

```
S: Searchable
I: case insensitive
C: encrypted
```

To create a table:

```
% nistbladm -c table-type column-spec .... table-name
```

For example, to create a table of type *computers* and of name *computers.example.com.*, with two columns, *name* and *model*, which are both searchable, you would use the following command:

```
% nistbladm -c computers name=S model=S computers.example.com.
```

(assuming your domain_name is example.com)

To delete a table:

```
% nistbladm -d table-name
```

For example, to delete your computer's table, you would use the following command:

```
% nistbladm -d computers.example.com.
```

For more information about adding entries or modifying entires, refer to the *nistbladm* man page.

6.3.14 How to Examine NIS+ tables.

The *niscat* command displays the contents of NIS+ tables.

To display the object properties of a table:

```
% niscat -o table-name
```

or:

```
% niscat -o entry
```

To display the contents of a table:

```
% niscat -h table-name
```

6.3.15 How to Modify NIS+ Tables.

NIS+ tables may be modified in a number of ways. One note for all of these methods is that a NIS+ principal must be a member of the admin NIS+ group to make modifications to most tables (see Section 6.3.8).

The best method is to use the *admintool* GUI to modify them. The only disadvantages to this approach are: *admintool* requires X to be running; not all the standard tables are available through *admintool*; and new tables will never be available through *admintool*.

If you can not use *admintool* to modify a table, *nisaddent* is the best alternative. The *nisaddent* command loads information from text files or from NIS maps into NIS+ tables. It can also dump the contents of the NIS+ tables back to text files. The following options are used along with the *nisaddent* command:

- a append:** add the contents of the source to the table
- r replace:** substitute contents of the source for the contents of the table
- m merge:** merge the contents of the source with the contents of the table.
- d dump:** dump the contents of the table to stdout

(With no -a, -r or -m options, the default is REPLACE)

You can put new entries into a file, and then merge in those changes:

```
% nisaddent -m -f filename table-type
```

For example:

```
% nisaddent -m -f /etc/hosts hosts
```

Or, you could dump a table, make changes, and then replace the copy of the table in NIS+

For example:

```
% nisaddent -d hosts > /tmp/hosts  
% vi /tmp/hosts  
% nisaddent -r -f /etc/hosts hosts
```

There is a special case to modify the password table using *nisaddent*.

Example:

```
% nisaddent -d passwd > /tmp/passwd  
% nisaddent -d shadow > /tmp/shadow  
% vi /tmp/passwd  
% nisaddent -r -f /tmp/passwd passwd  
% nisaddent -m -f /tmp/shadow -t passwd.org_dir shadow
```

The reason that you must do the *passwd* table this way is that if you don't reload all the shadow information, your passwords will be lost.

If you do not want to use *nisaddent*, your final option is to use *nistbladm* to directly modify the table. This can be fairly complex. Examine the *nistbladm* man page for more information on how to do this.

6.3.16 How to Regularly Administer NIS+. Depending on the updates one performs in the namespace, it is a good idea to frequently perform *nisping -C* so that log files get written to the disk. You may wish to put this into a cron tab on your root-master server, to make sure that it is executed daily.

Another important NIS+ administration task is to regularly back up */var/nis*, to make sure that you can recover in the case of a massive failure.

6.3.17 How to Remove NIS+. If you wish to remove NIS+, you should run the following commands on all of your NIS+ machines:

```
# cp /etc/nsswitch.files /etc/nsswitch.conf
# /etc/init.d/rpc stop
# rm -f /etc/.rootkey
# rm -rf /var/nis/*
# rm -f /etc/defaultdomain
# /etc/init.d/rpc start
```

It is suggested that you start with the clients, and do the servers last.

6.3.18 How to define the printer table in NIS+. Run the following command, as *root*, to set up the NIS+ printers table definition:

```
# nistbladm -c -D access=n+r,o+rmcd,g+rmcd,w+r printers
printer_name=S,o+rmcd,g+r,w+r printer_host=S,o+rmcd,g+r,w+r
description=,o+rmcd,g+r,w+r printers.org_dir.`domainname`.
```

Once you have set up this definition, you can confirm the permissions are set properly:

```
# niscat -o printers.org_dir
Object Name      : printers
Owner            : ppp.hans.com.
Group            : admin.hans.com.
Domain           : org_dir.hans.com.
Access Rights    : r---rmcdrmcd---
Time to Live     : 12:0:0
Object Type      : TABLE
Table Type       : printers
Number of Columns : 3
Character Separator :
Search Path      :
Columns          :
[0]      Name      : printer_name
Attributes       : (SEARCHABLE, TEXTUAL DATA, CASE SENSITIVE)
```

```
Access Rights : ----rmcdr---r---  
[1]      Name : printer_host  
Attributes  : (SEARCHABLE, TEXTUAL DATA, CASE SENSITIVE)  
Access Rights : ----rmcdr---r---  
[2]      Name : description  
Attributes   : (TEXTUAL DATA)  
Access Rights : ----rmcdr---r---
```

After this, *admintool* or the *nisaddent* command can be used to populate the Printers table.

6.4 Some Frequently Asked Questions

6.4.1 Miscellaneous Questions

Q1: What are the main features of NIS+?

Q2: What new functionality does NIS+ have?

Q3: What are the differences between NIS and NIS+?

A: NIS name space is a flat namespace, which means that it does not support subdomains. Under NIS, only one domain is accessible from a given host. In NIS+, the namespace is hierarchical. This hierarchical structure is similar to the Unix filesystem structure. Since the NIS+ namespace is hierarchical, it can be configured to conform with the logical hierarchy of the organization. This means that you can create subdomains for different levels of organization.

In NIS, even for a small change in the map, the master server needs to push the whole map to the slave servers. However, in NIS+, the database updates are incremental. This means that only changes in the map are replicated to replica servers. Therefore, NIS+ database updates are more efficient and less time-consuming.

Another important difference between NIS and NIS+ is server binding. In NIS, clients are hard-bound to a specific server. During the bootup time, the *ypbind* process on the client side binds to a specific server. However, the NIS+ client library is not a separate process. In NIS, the *ypwhich* command can tell you to which specific server the client is bound to, but that is not possible in NIS+. In other words, the binding in NIS+ is soft binding.

NIS maps can be searched by only one predefined searchable column. NIS+ tables allow more than one searchable column.

NIS supports UNIX groups and netgroups. NIS+ also supports the concept of NIS+ group. One or more NIS+ users can be grouped together into a NIS+ group. Multiple NIS+ groups can be defined, each with different access and modification rights to the NIS+ namespace.

NIS+ also has much improved security.

NIS does not support authentication, authorization and secure RPC, whereas NIS+ supports authentication, authorization and secure RPC.

Q: What is my network password?

A: In most cases, your network password should be the same as your log-in password. When NIS+ is just getting set up, network passwords are often set to 'nisplus'.

Q: Why can't I have machines and users with the same name?

A: All machines and users must have credentials created for them. If you have a machine and a user with the same name, only one of them will be able to have credentials. In case of a naming conflict of this sort, you should change the machine's name you may have to recreate credentials for the user and machine afterwards:

```
% nisclient -c user
% nisclient -c machine
```

6.4.2 NIS+ Setup Problems

Q: Why does *nisserv* fail when I run it, as described in Section 6.3.4?

A: If for some reason the *nisserv* script fails, check the error message. It will give some ideas about the failure. Another option is to do the configuration manually using *nisinit*, and *nissetup*, as is described in the *Name Services Administration Guide*. This will give an idea about which step the script is failing in. This can help to diagnose the problem better. If the *nisinit -r* step hangs, then check if you are running DNI. The DNI installation modifies */etc/netconfig* file with this line:

```
nsp    tpi_cots_ord    -    decnet    nsp    /dev/nsp
/usr/lib/straddr.so
```

If you comment this line out and then run the script again, it will work correctly.

6.4.3 User Log-in Problems

Q: Why do I get the following error on log-in:

"Password does not decrypt secret key for ..."

A: This means that the user's log-in password and network password do not match. After log-in, the user must run *keylogin* to get NIS+ credentials:

% keylogin

They will have to type their NIS+ network password at the *keylogin* prompt. This may very well be 'nisplus' if the user is logging in for the first time. Afterwards, the user should run *chkey*, to synch the log-in and network passwords:

% chkey -p

Users have to again type their NIS+ password (nisplus) and then their log-in password (password typed in when logging into system).

Q: Why do I get the following error on login:

```
"/usr/bin/passwd: <user> does not exist"  
"Connection closed by foreign host."
```

A1: This can be the result of selecting "cleared until first login" in *admintool*, when you initially create a user. You should instead select a normal password for a user when you create the user's account.

A2: If you are trying to use password aging, you must install the password aging point patch.

6.4.4 NIS+ Lookup Problems

Q: Why do I get inconsistent results when I do certain NIS+ lookups?

A: In NIS+, the server binding is a soft binding. That is, every query may be accessing a different server. Therefore, if a replica is not in synch with the master, clients will get inconsistent information for every query. When you get inconsistent information for queries run the *snoop* command (see Section 6.2.3) to find out which server is providing the incorrect information.

6.5 References

6.5.1 Important Man Pages

chkey
keylogin
newkey
nis
nis_cachemgr
nisaddcred

niscat
nisaddent
nischgrp
nischown
nischttl
nisclient
nisdefaults
nisgrep
nisgrpadm
nisinit
nislog
nisl
nismatch
nismkdir
nisping
nispopulate
nism
nismkdir
nisserver
nistbladm
nisudpkeys
rpc.nisd

6.5.2 Sunsolve Documents. There are a number of Sunsolve documents concerning NIS+. The ones listed below either contain some additional information not in this document, or reference rare problems, or rare how-tos.

6.5.2.1 FAQs

1012 NIS+ questions

6.5.2.2 Infodocs

2216 NIS+ questions
11742 How to convert a NIS+ root replica server to a root mas

6.5.2.3 SRDBs

5874 nis+ database recovery
6285 Change of root passwd on NIS+ server breaks authenticat
6487 Differences between NIS and NIS+
6640 Why does NIS+ require passwords
6616 Is it possible to revert to NIS
7202 Cannot change NIS passwords served by NIS+ servers
10448 Changing the NIS+ master server.
10941 NIS+ error messages
10951 NIS+ servers unreachable
11728 Changing a NIS+ server's IP address.

6.5.3 Sun Educational Services. NIS+ concepts and administration

offered by SUNED.

6.5.4 Solaris Documentation

Name Services Administration Guide, part #801-6633-10
Name Services Configuration Guide, part #801-6635-10

6.5.5 Third Party Documentation

All About Administering NIS+, by Rick Ramasey, Prentice Hall

6.5.6 RFCs. There are no RFCs on NIS+.

6.6 Supportability

SunService is not responsible for the initial configuration of your NIS+ environment. In addition, SunService can not diagnose your NIS+ performance problems, or suggest NIS+ tuning guidelines. We can help resolve problems where NIS+ is not behaving correctly, but in such cases the contact must be a system administrator who understands how the NIS+ domain is set up.

6.7 Additional Support

For initial configuration, or NIS+ performance tuning guidelines, please contact your local SunService office for possible consulting offerings. Sun's Customer Relations organization can put you in touch with your local SunIntegration or Sales office. You can reach Customer Relations at 1-800-821-4643.

SECTION 7. MAIL ADMINISTRATION

7.1 Introduction

Sendmail implements a general purpose internetwork mail routing facility under the UNIX operating system. It is not tied to any one transport protocol. Its function may be likened to a crossbar switch, relaying messages from one domain into another. In the process, it can do a limited amount of message header editing to put the message into a format that is appropriate for the receiving domain. All of this is done under the control of a configuration file.

Due to the requirements of flexibility for *sendmail*, the configuration can seem somewhat unapproachable. However, for most GCCS SIPRNET sites, the only difference in the *sendmail.cf* file is the domain name. Those sites having unique address resolution rules will have to address those individually.

The GCCS COE Kernel tape configures each platform for mail according to how certain questions are answered.

- g. If it was stated that the platform is a mail server (mail host) during the installation of the GCCS COE Kernel (see Section 4.3 of the *GCCS Implementation Procedures*), the following occurs:
 - 1. A preconfigured *main.cf* file* is configured with the site's domain name and copied into the */etc/mail/sendmail.cf* file.
 - 2. An alias of *mailhost* is added after the site's host name in the */etc/host* file.
 - 3. The file system */var/mail* is exported.
- b. If it was stated that the platform is not a mail server, the following occurs:
 - 1. The preconfigured *subsidiary.cf* file is configured with the site's domain name and copied into the */etc/mail/sendmail.cf* file.
 - 2. An IP address with an alias of *mailhost* is added to the host table of that platform.
 - 3. The */var/mail* file system of the mail server is mounted.

* Copies of these mail administration files are provided in Section 7.2, with bold print used to identify fields that were modified.

- c. The `/usr/lib/sendmail.mx` file is copied to `/usr/lib/sendmail` to enable mail to use DNS.

Although *sendmail* is intended to run without the need for monitoring, it has a number of features that may be used to monitor or adjust the operation under unusual circumstances. These features are not described in this document. The following list of documents are recommended for those who would like more detailed information on the operation of *sendmail*:

sendmail - by Bryan Costales with Eric Allman & Neil Rickert, published by O'Reilly & Associates.

sendmail - An Internetwork Mail Router, by Eric Allman (SMM-16)

sendmail - Installation and Operation Guide, by Eric Allman (SMM-07).

Other useful documents are the following Requests for Comments (RFCs):

RFC822	Standard for the Format of ARPA-Internet Text Messages
RFC821	Simple Mail Transfer Protocol
RFC819	The Domain naming Convention for Internet User Applications
RFC1123	Requirements for Internet hosts - Application and Support.

To receive these RFCs via electronic mail:

mail service@rs.internic.net
help

or

mail service@rs.internic.net
send RFC 822

7.2 Mail Administration Files

```
#####  
#  
#   Sendmail configuration file for "MAIN MACHINES"  
#  
#   You should install this file as /etc/sendmail.cf  
#   if your machine is the main (or only) mail-relaying  
#   machine in your domain. Then edit the file to  
#   customize it for your network configuration.  
#  
#   See the manual "System and Network Administration for the Sun  
#   Workstation". Look at "Setting Up The Mail Routing System" in  
#   the chapter on Communications. The Sendmail reference in the  
#   back of the manual is also useful.  
#
```

```

#      @(#)main.mc 1.17 90/01/04 SMI
#

###   local info

# delete the following if you have no sendmailvars table
Lmmaildomain

# my official hostname
# You have two choices here.  If you want the gateway machine to identify
# itself as the DOMAIN, use this line:
Dj$m
# If you want the gateway machine to appear to be INSIDE the domain, use:
#Dj$w.$m
# if you are using sendmail.mx (or have a fully-qualified hostname), use:
#Dj$w

# major relay mailer - typical choice is "ddn" if you are on the
# Defense Data Network (e.g. Arpanet or Milnet)
#DMsmartuucp
DMddn

# major relay host: use the $M mailer to send mail to other domains
#DR ddn-gateway
#CR ddn-gateway
DR mailhost
CR mailhost

# If you want to pre-load the "mailhosts" then use a line like
# FS /usr/lib/mailhosts
# and then change all the occurrences of $%y to be $=S instead.
# Otherwise, the default is to use the hosts.byname map if NIS
# is running (or else the /etc/hosts file if no NIS).

# valid top-level domains (default passes ALL unknown domains up)
CT arpa com edu gov mil net org smil
CT us de fr jp kr nz il uk no au fi nl se ca ch my dk ar

# options that you probably want on a mailhost:

# checkpoint the queue after this many recipients
OC10

# refuse to send tiny messages to more than these recipients
Ob10

#####
#
#      General configuration information

# local domain names
#
# These can now be determined from the domainname system call.
# The first component of the NIS domain name is stripped off unless

```

```

# it begins with a dot or a plus sign.
# If your NIS domain is not inside the domain name you would like to have
# appear in your mail headers, add a "Dm" line to define your domain name.
# The Dm value is what is used in outgoing mail. The Cm values are
# accepted in incoming mail. By default Cm is set from Dm, but you might
# want to have more than one Cm line to recognize more than one domain
# name on incoming mail during a transition.
# Example:
# DmCS.Podunk.EDU
# Cm cs cs.Podunk.EDU
#

```

```

DmDUMMY.
Cm DUM DUMMY.

```

```

# known hosts in this domain are obtained from gethostbyname() call

# Version number of configuration file
#ident    "@(#)version.m4      1.17  92/07/14 SMI"      /* SunOS 4.1      */
#
#
#      Copyright Notice
#
#Notice of copyright on this source code product does not indicate
#publication.
#
#      (c) 1986,1987,1988,1989  Sun Microsystems, Inc
#
#      All rights reserved.

```

DVSMI-SVR4

Standard macros

```

# name used for error messages
DnMailer-Daemon
# special user
CDMailer-Daemon root daemon uucp
# UNIX header format
DlFrom $g $d
# delimiter (operator) characters
Do.:%@!^=/[ ]
# format of a total name
Dq$g$?x ($x)$ .
# SMTP login message
De$j Sendmail $v/$V ready at $b

```

Options

```

# Remote mode - send through server if mailbox directory is mounted
OR
# location of alias file
OA/etc/mail/aliases
# default delivery mode (deliver in background)
Odbackground
# rebuild the alias file automagically

```

```
OD
# temporary file mode -- 0600 for secure mail, 0644 for permissive
OF0600
# default GID
Og1
# location of help file
OH/etc/mail/sendmail.hf
# log level
OL9
# default messages to old style
Oo
# Cc my postmaster on error replies I generate
OPPostmaster
# queue directory
OQ/var/spool/mqueue
# read timeout for SMTP protocols
Or15m
# status file -- none
OS/etc/mail/sendmail.st
# queue up everything before starting transmission, for safety
Os
# return queued mail after this long
OT3d
# default UID
Oul

### Message precedences
Pfirst-class=0
Pspecial-delivery=100
Pjunk=-100

### Trusted users
T root daemon uucp

### Format of headers
H?P?Return-Path: <$g>
HReceived: $?sfrom $s $.by $j ($v/$V)
        id $i; $b
H?D?Resent-Date: $a
H?D?Date: $a
H?F?Resent-From: $q
H?F?From: $q
H?x?Full-Name: $x
HSubject:
H?M?Resent-Message-Id: <$t.$i@$j>
H?M?Message-Id: <$t.$i@$j>
HErrors-To:

#####
### Rewriting rules ###
#####

# Sender Field Pre-rewriting
S1
# None needed.
```



```

# Recipient Field Pre-rewriting
S2
# None needed.

# Name Canonicalization

# Internal format of names within the rewriting rules is:
#   anything<@host.domain.domain...>anything
# We try to get every kind of name into this format, except for local
# names, which have no host part. The reason for the "<>" stuff is
# that the relevant host name could be on the front of the name (for
# source routing), or on the back (normal form). We enclose the one that
# we want to route on in the <>'s to make it easy to find.
#
S3

# handle "from:<>" special case
R$*<>$*                $$@                turn into magic token

# basic textual canonicalization
R$*<$+>$*                $2
    basic RFC822 parsing

# make sure <a,@b,@c:user@d> syntax is easy to parse -- undone later
R@$$+, $+:$+            @$1:$2:$3            change all ", " to ":"
R@$$+:$+                @$>6<@$1>:$2            src route canonical

R$+:$*;$+                @$1:$2;$+                list syntax
R$+@$+                $:$1<@$2>                focus on domain
R$+<$+@$+>                $1$2<@$3>                move gaze right
R$+<@$+>                @$>6$1<@$2>                already canonical

# convert old-style names to domain-based names
# All old-style names parse from left to right, without precedence.
R$-!$+                @$>6$2<@$1.uucp>            uucphost!user
R$-.$+!$+                @$>6$3<@$1.$2>            host.domain!user
R$+%$+                @$>3$1@$2                user%host

# Final Output Post-rewriting
S4
R$+<@$+.uucp>                $2!$1
u@h.uucp => h!u
R$+                $: $>9 $1                Clean up addr
R$*<$+>$*                $1$2$3
defocus

# Clean up an name for passing to a mailer
# (but leave it focused)
S9
R$=w!@                $$w!$n
R@                @$n                handle <> error addr
R$*<$*LOCAL>$*                $1<$2$m>$3            change local info
R<@$+>$*:$+:$+                <@$1>$2,$3:$4            <route-addr> canonical

#####

```

```
# Rewriting rules

# special local conversions
S6
R$*<@$*$=m>$*          $1<@$2LOCAL>$4          convert local domain

# Local and Program Mailer specification

Mlocal, P=/bin/mail, F=flsSDFMmnP, S=10, R=20, A=mail -d $u
Mprog,  P=/bin/sh,   F=lsDFMeuP,  S=10, R=20, A=sh -c $u

S10
# None needed.

S20
# None needed.

#ident    "@(#)etherm.m4 1.15  93/04/05 SMI"      /* SunOS 4.1      */
#
#      Copyright Notice
#
#Notice of copyright on this source code product does not indicate
#publication.
#
#      (c) 1986,1987,1988,1989  Sun Microsystems, Inc
#      All rights reserved.

#####
#####
#####      Ethernet Mailer specification
#####
##### Messages processed by this configuration are assumed to remain
##### in the same domain.  This really has nothing particular to do
##### with Ethernet - the name is historical.

Mether, P=[TCP], F=msDFMuCX, S=11, R=21, A=TCP $h
S11
R$*<@$+>$*          $$1<@$2>$3          already ok
R$=D                $$1<@$w>            tack on my hostname
R$+                 $$1<@$k>            tack on my mbox hostname

S21
R$*<@$+>$*          $$1<@$2>$3          already ok
R$+                 $$1<@$k>            tack on my mbox hostname

#####
# General code to convert back to old style UUCP names
S5
R$+<@LOCAL>          @$ $w!$1
name@LOCAL => sun!name
R$+<@$-.LOCAL>        @$ $2!$1
u@h.LOCAL => h!u
R$+<@$+.uucp>          @$ $2!$1
u@h.uucp => h!u
R$+<@$*>              @$ $2!$1          u@h => h!u
```

```
# Route-addr's do not work here.  Punt til uucp-mail comes up with something.
R<@$+>$*          $@ @$1$2          just defocus and punt
R$*<$*>$*          $@ $1$2$3         Defocus strange stuff

#      UUCP Mailer specification

Muucp,    P=/usr/bin/uux, F=msDFMhuU, S=13, R=23,
          A=uux - -r -a$f $h!rmail ($u)

# Convert uucp sender (From) field
S13
R$+          $:$>5$1
convert to old style
R$=w!$+      $2
          strip local name
R$+          $:$w!$1          stick on real host name

# Convert uucp recipient (To, Cc) fields
S23
R$+          $:$>5$1
convert to old style

#ident    "@(#)ddnm.m4    1.8    93/06/30 SMI"    /* SunOS 4.1    */
#
#
#      Copyright Notice
#
#Notice of copyright on this source code product does not indicate
#publication.
#
#      (c) 1986,1987,1988,1989  Sun Microsystems, Inc
#      All rights reserved.

#####
#
#      DDN Mailer specification
#
#      Send mail on the Defense Data Network
#      (such as Arpanet or Milnet)

Mddn, P=[TCP], F=msDFMuCX, S=22, R=22, A=TCP $h, E=\r\n

# map containing the inverse of mail.aliases
# Note that there is a special case mail.byaddr will cause reverse
# lookups in both Nis+ and NIS.
# If you want to use ONLY Nis+ for alias inversion comment out the next line
# and uncomment the line after that
DZmail.byaddr
#DZREVERSE.mail_aliases.org_dir

S22
R$*<@LOCAL>$*          $:$1
R$-<@$->          $:$>3${Z$1@$2$}          invert aliases
R$*<@$+.$*>$*          $@$1<@$2.$3>$4          already ok
```

```

R$+<@$+>$*          @$1<@$2.$m>$3          tack on our domain
R$+                  @$1<@$w.$m>          tack on our full name

# "Smart" UUCP mailer: Uses UUCP transport but domain-style naming
Msmartuucp, P=/usr/bin/uux, F=CmsDFMhuU, S=22, R=22,
    A=uux - -r $h!rmail ($u)

#####
#
#      RULESET ZERO
#
#      This is the ruleset that determines which mailer a name goes to.

# Ruleset 30 just calls rulesets 3 then 0.
S30
R$*          $: $>3 $1          First canonicalize
R$*          @$ $>0 $1          Then rerun ruleset 0

S0
# On entry, the address has been canonicalized and focused by ruleset 3.
# Handle special cases.....
R@          $#local $:$n          handle <> form

# resolve the local hostname to "LOCAL".
R$*<$*$=w.LOCAL>$*          $1<$2LOCAL>$4
thishost.LOCAL
R$*<$*$=w.uucp>$*          $1<$2LOCAL>$4
thishost.uucp
R$*<$*$=w>$*          $1<$2LOCAL>$4          thishost

# Mail addressed explicitly to the domain gateway (us)
R$*<@LOCAL>          @$>30$1          strip our name, retry
R<@LOCAL>:$+          @$>30$1          retry after route strip

# For numeric spec, you can't pass spec on to receiver, since old rcvr's
# are not smart enough to know that [x.y.z.a] is their own name.

R<@[$+]>:$*          $:$>9 <@[$1]>:$2          Clean it up, then...
R<@[$+]>:$*          $#ether @$[$1] $:$2          numeric internet spec
R<@[$+]>,$*          $#ether @$[$1] $:$2          numeric internet spec
R$*<@[$+]>          $#ether @$[$2] $:$1          numeric internet spec

# deliver to known ethernet hosts explicitly specified in our domain

R$*<@$%y.LOCAL>$*          $#ether @$2 $:$1<@$2>$3
user@host.sun.com
# deliver to hosts in our domain that have a MX recod
R$*<@$%x.LOCAL>$*          $#ether @$2 $:$1<@$2>$3
user@host.sun.com

# etherhost.uucp is treated as etherhost.$m for now.
# This allows them to be addressed from uucp as foo!sun!etherhost!user.
R$*<@$%y.uucp>$*          $#ether @$2 $:$1<@$2>$3
user@etherhost.uucp

```

```
# Explicitly specified names in our domain -- that we've never heard of
R$*<@$*.LOCAL>$*          $error $:Never heard of host $2 in domain $m

# Clean up addresses for external use -- kills LOCAL, route-addr ,=>:
R$*                        $:>9 $1
    Then continue...

# resolve UUCP-style names
R<@$-.uucp>:$+              $#uucp      @$ $1 $:$2
    @host.uucp:...
R$+<@$-.uucp>              $#uucp      @$ $2 $:$1
    user@host.uucp

# Pass other valid names up the ladder to our forwarder
R$*<@$*.$=T>$*             $#M          @$R $:$1<@$2.$3>$4
user@domain.known

# Replace following with above to only forward "known" top-level domains
R$*<@$*.$+>$*              $#M          @$R $:$1<@$2.$3>$4
user@any.domain

# if you are on the DDN, then comment-out both of the the lines above
# and use the following instead:
R$*<@$*.$+>$*              $#ddn        @$ $2.$3 $:$1<@$2.$3>$4
user@any.domain

# All addresses in the rules ABOVE are absolute (fully qualified domains).
# Addresses BELOW can be partially qualified.

# deliver to known ethernet hosts
R$*<@$%y>$*                $#ether @$ $2 $:$1<@$2>$3      user@etherhost
# deliver to known ethernet hosts that has MX record
R$*<@$%x>$*                $#ether @$ $2 $:$1<@$2>$3      user@etherhost

# other non-local names have nowhere to go; return them to sender.
R$*<@$+.$->$*              $error $:Unknown domain $3
R$*<@$+>$*                $error $:Never heard of $2 in domain $m
R$*@$*                    $error $:I don't understand $1@$2

# Local names with % are really not local!
R$+%$+                    @$>30$1@$2                      turn % => @, retry

# everything else is a local name
R$+                        $#local $:$1                    local names

#####
#
#     SENDMAIL CONFIGURATION FILE FOR SUBSIDIARY MACHINES
#
#     You should install this file as /etc/sendmail.cf
#     if your machine is a subsidiary machine (that is, some
#     other machine in your domain is the main mail-relaying
#     machine). Then edit the file to customize it for your
#     network configuration.
```

```
#
#      @(#)subsidiary.mc 1.11 88/02/08 SMI; from UCB arpa.mc 3.25 2/24/83
#

# delete the following if you have no sendmailvars table
Lmmaildomain

# local UUCP connections -- not forwarded to mailhost
CV

# my official hostname
Dj$w.$m

# major relay mailer
DMddn

# major relay host
DRmailhost
CRmailhost

#####
#
#      General configuration information

# local domain names
#
# These can now be determined from the domainname system call.
# The first component of the NIS domain name is stripped off unless
# it begins with a dot or a plus sign.
# If your NIS domain is not inside the domain name you would like to have
# appear in your mail headers, add a "Dm" line to define your domain name.
# The Dm value is what is used in outgoing mail. The Cm values are
# accepted in incoming mail. By default Cm is set from Dm, but you might
# want to have more than one Cm line to recognize more than one domain
# name on incoming mail during a transition.
# Example:
# DmCS.Podunk.EDU
# Cm cs cs.Podunk.EDU
#
# known hosts in this domain are obtained from gethostbyname() call

DmDUMMY.
Cm DUM DUMMY.

# Version number of configuration file
#ident      "@(#)version.m4      1.17  92/07/14 SMI"      /* SunOS 4.1      */
#
#
#      Copyright Notice
#
#Notice of copyright on this source code product does not indicate
#publication.
#
#      (c) 1986,1987,1988,1989  Sun Microsystems, Inc
```

All rights reserved.

DVSMI-SVR4

Standard macros

name used for error messages
DnMailer-Daemon
specail user
CDMailer-Daemon root daemon uucp
UNIX header format
DlFrom \$g \$d
delimiter (operator) characters
Do.:%@!^=/[]
format of a total name
Dq\$g\$?x (\$x)\$.
SMTP login message
De\$j Sendmail \$v/\$V ready at \$b

Options

Remote mode - send through server if mailbox directory is mounted
OR
location of alias file
OA/etc/mail/aliases
default delivery mode (deliver in background)
Odbackground
rebuild the alias file automatically
OD
temporary file mode -- 0600 for secure mail, 0644 for permissive
OF0600
default GID
Ogl
location of help file
OH/etc/mail/sendmail.hf
log level
OL9
default messages to old style
Oo
Cc my postmaster on error replies I generate
OPPostmaster
queue directory
OQ/var/spool/mqueue
read timeout for SMTP protocols
Or15m
status file -- none
OS/etc/mail/sendmail.st
queue up everything before starting transmission, for safety
Os
return queued mail after this long
OT3d
default UID
Oul

Message precedences

```

Pfirst-class=0
Pspecial-delivery=100
Pjunk=-100

###   Trusted users
T root daemon uucp

###   Format of headers
H?P?Return-Path: <$g>
HReceived: $?sfrom $s $.by $j ($v/$V)
        id $i; $b
H?D?Resent-Date: $a
H?D?Date: $a
H?F?Resent-From: $q
H?F?From: $q
H?x?Full-Name: $x
HSubject:
H?M?Resent-Message-Id: <$t.$i@$j>
H?M?Message-Id: <$t.$i@$j>
HErrors-To:

#####
###   Rewriting rules   ###
#####

#   Sender Field Pre-rewriting
S1
# None needed.

#   Recipient Field Pre-rewriting
S2
# None needed.

# Name Canonicalization

# Internal format of names within the rewriting rules is:
#   anything<@host.domain.domain...>anything
# We try to get every kind of name into this format, except for local
# names, which have no host part. The reason for the "<>" stuff is
# that the relevant host name could be on the front of the name (for
# source routing), or on the back (normal form). We enclose the one that
# we want to route on in the <>'s to make it easy to find.
#
S3

# handle "from:<>" special case
R$*<>$*                $$@                turn into magic token

# basic textual canonicalization
R$*<$+>$*                $2
        basic RFC822 parsing

# make sure <a,@b,@c:user@d> syntax is easy to parse -- undone later
R@$+,$+:$+                @$1:$2:$3                change all ",", to ":"
R@$+:$+                @$>6<@$1>:$2                src route canonical
  
```



```

R$+:$*;$+      @$1:$2;$3      list syntax
R$+@$+         $:$1<@$2>       focus on domain
R$+<$+@$+>     $1$2<@$3>      move gaze right
R$+<@$+>       @$>6$1<@$2>    already canonical

# convert old-style names to domain-based names
# All old-style names parse from left to right, without precedence.
R$-!$+         @$>6$2<@$1.uucp> uucphost!user
R$-.$+!$+      @$>6$3<@$1.$2>   host.domain!user
R$+%$+         @$>3$1@$2       user%host

# Final Output Post-rewriting
S4
R$+<@$+.uucp>   $2!$1
u@h.uucp => h!u
R$+             $: $>9 $1      Clean up addr
R$*<$+>$*      $1$2$3
defocus

# Clean up an name for passing to a mailer
# (but leave it focused)
S9
R$=w!@          @$w!$n
R@              @$n           handle <> error addr
R$*<$*LOCAL>$*  $1<$2$m>$3     change local info
R<@$+>$*:$+:$+ <@$1>$2,$3:$4   <route-addr> canonical

#####
# Rewriting rules

# special local conversions
S6
R$*<@$*$=m>$*   $1<@$2LOCAL>$4 convert local domain

# Local and Program Mailer specification

Mlocal, P=/bin/mail, F=flsSDFMmnP, S=10, R=20, A=mail -d $u
Mprog, P=/bin/sh, F=lsDFMeuP, S=10, R=20, A=sh -c $u

S10
# None needed.

S20
# None needed.

#ident "@(#)etherm.m4 1.15 93/04/05 SMI" /* SunOS 4.1 */
#
# Copyright Notice
#
#Notice of copyright on this source code product does not indicate
#publication.
#
# (c) 1986,1987,1988,1989 Sun Microsystems, Inc
# All rights reserved.

```

```
#####
#####
##### Ethernet Mailer specification
#####
##### Messages processed by this configuration are assumed to remain
##### in the same domain. This really has nothing particular to do
##### with Ethernet - the name is historical.

Mether, P=[TCP], F=msDFMuCX, S=11, R=21, A=TCP $h
S11
R$*<@$+>$*          $@$1<@$2>$3          already ok
R$=D                  $@$1<@$w>          tack on my hostname
R$+                   $@$1<@$k>          tack on my mbox hostname

S21
R$*<@$+>$*          $@$1<@$2>$3          already ok
R$+                   $@$1<@$k>          tack on my mbox hostname

#####
# General code to convert back to old style UUCP names
S5
R$+<@LOCAL>          $@ $w!$1
name@LOCAL => sun!name
R$+<@$-.LOCAL>       $@ $2!$1
u@h.LOCAL => h!u
R$+<@$+.uucp>        $@ $2!$1
u@h.uucp => h!u
R$+<@$*>             $@ $2!$1          u@h => h!u
# Route-addr's do not work here. Punt til uucp-mail comes up with something.
R<@$+>$*             $@ @$1$2          just defocus and punt
R$*<@$*>$*           $@ $1$2$3        Defocus strange stuff

# UUCP Mailer specification

Muucp, P=/usr/bin/uux, F=msDFMhuU, S=13, R=23,
A=uux - -r -a$f $h!rmail ($u)

# Convert uucp sender (From) field
S13
R$+                   $:$>5$1
convert to old style
R$=w!$+               $2
strip local name
R$+                   $:$w!$1          stick
on real host name

# Convert uucp recipient (To, Cc) fields
S23
R$+                   $:$>5$1
convert to old style

##### RULESET ZERO PREAMBLE

# Ruleset 30 just calls rulesets 3 then 0.
```

```

S30
R$*          $: $>3 $1          First canonicalize
R$*          @$ $>0 $1          Then rerun ruleset 0

S0
# On entry, the address has been canonicalized and focused by ruleset 3.
# Handle special cases.....
R@          $#local $:$n          handle <> form
# Earlier releases special-cased the [x.y.z.a] format, but SunOS 4.1 or later
# should handle these properly on input.

# now delete redundant local info
R$*<$*=w.LOCAL>$*          $1<$2>$4
thishost.LOCAL
R$*<@LOCAL>$*          $1<@$m>$2          host == domain gateway
R$*<$*=w.uucp>$*          $1<$2>$4
thishost.uucp
R$*<$*=w>$*          $1<$2>$4
thishost

# arrange for local names to be fully qualified
R$*<@$%1>$*          $1<@$2.LOCAL>$3          user@etherhost

# For numeric spec, you can't pass spec on to receiver, since old rcvr's
# were not smart enough to know that [x.y.z.a] is their own name.
R<@[$+]>:$*          $:$>9 <@[$1]>:$2          Clean it up, then...
R<@[$+]>:$*          $#ether @$[$1] $:$2          numeric internet spec
R<@[$+]>,$*$          $#ether @$[$1] $:$2          numeric internet spec
R$*<@[$+]>          $#ether @$[$2] $:$1          numeric internet spec

R$*<$*.$>$*          $1<$2>$3          drop trailing dot
R<@>:$*          @$>30$1          retry after route strip
R$*<@>          @$>30$1          strip null trash & retry

#####
### Machine dependent part of ruleset zero ###
#####

# resolve names we can handle locally
R<@$=V.uucp>:$+          $:$>9 $1          First clean up, then...
R<@$=V.uucp>:$+          $#uucp @$ $1 $:$2          @host.uucp:...
R$+<@$=V.uucp>          $#uucp @$ $2 $:$1          user@host.uucp

# optimize names of known ethernet hosts
R$*<@$%1.LOCAL>$*          $#ether @$ $2 $:$1<@$2>$3          user@host.here
# local host that has a MX record
R$*<@$%x.LOCAL>$*          $#ether @$ $2 $:$1<@$2>$3          user@host.here

# other non-local names will be kicked upstairs
R$+          $:$>9 $1          Clean up, keep <>
R$*<@$+>$*          $#M @$R $:$1<@$2>$3          user@some.where
R$*@$*          $#M @$R $:$1<@$2>          strangeness with @

# Local names with % are really not local!
R$+@$+          @$>30$1@$2          turn % => @, retry

```

```
# everything else is a local name
R$+                $#local $:$1          local names

# Ruleset 33 is used in remote mode only
S33
R$+<@$=w.LOCAL>    $1
R$+<@$=w>          $1
R$*<@$+>$*         $#ether $@$k $:$1<@$2>$3  forward to $k
R$+                $#local $:$1          local names
```

SECTION 8. PRINTER ADMINISTRATION

8.1 Scope

This section addresses the installation of the SUN NeWSprint product on those SUNservers that must support SUN printers, and the use of the Network Printer Administration Application provided with GCCS Version 2.2.

8.2 Installing NeWSprint on Print Servers

Any SUNserver or SUNstation that has a SUN printer directly attached to it requires NeWSprint to use that printer. GCCS is currently using the following SUN printers: SPARCprinter, NeWSprinter20, and SPARCprinter II. For the SPARCprinter and the NeWSprinter20, NeWSprint is provided on a CD labeled "NeWSprint Version 2.5 revision b." For the SPARCprinter II, NeWSprint is provided on a CD labeled "Printer Manager Software V1.0 for Solaris 2.X." If a site attempts to install it after NIS+ has been activated, it will encounter problems. Prior to installing NeWSprint the site should obtain a NeWSprint font license. Execute the following steps to install NeWSprint:

- a. Log on to the print server as **root**.
- b. Insert the NeWSprint CD into the CD drive.

For SPARCprinterII use the CD "Print Manager Software V1.0 for Solaris 2.X."

For SPARCprinter/NeWSprinter20 use the CD "NeWSprint Version 2.5 revision b."

- c. Enter the following commands:

```
cd /cdrom/unnamed_cdrom<return>
cd sp2<return>    for SPARCprinterII only
./npcdm<return>
```

- d. A list of options is displayed. Choose **Option 1: Select Application**.

- e. A list of options is displayed. Choose the appropriate option.

```
SPARCprinter if using SPARCprinter
NeWSprinter20 if using NeWSprinter20
SPARCprinterII if using SPARCprinterII
NeWSprint if just installing NeWSprint software.
```

- f. Another list of options is displayed. Choose **Option 3: Install Application.**
- g. A series of questions and directions is displayed. Answer the questions and directions as follows:

Question: Begin Installation (y/n?)
Answer: **y**<return>

Press space bar two times to read more license information.

Question: Do you want to continue (y/n?)
Answer: **y**<return>

Question: Do you want to install NeWSprint Answerbook (y/n?)
Answer: **y**<return>

The following item(s) will be installed in /opt/NeWSprint:

NeWSprint

Continue (y/n?) **y** <return>

Question: What name do you want for the printer?
Answer: {Whatever name you wish for your printer} <return>

Question: Do you want this printer to be the default printer (y/n?)

Answer: **y** or **n** <return>

Question: Do you want to install NeWSprint font license (y/n?)
Answer: **y**<return>

Question: Enter NeWSprint font license:
Answer: Enter the license provided (Reference Section 10.3)

NeWSprint is now installed. SUN patch 102113-03 is required to prevent NeWSprint from locking up after printing one job. This patch is placed in /opt after the *load_patches* script is executed during the loading of the GCCS COE Kernel (Section 4.1 of Implementation Procedures). To install the patch, execute the following:

- a. Shut down the print scheduler with the following command (there is no need to be in single-user mode to load this patch):

lpshut<return>

- b. Install patch 102113-03 according to the steps in the README.102113-03 file provided

with the patch.

```
/opt/102113-03/installpatch /opt/102113-03<return>
```

c. Restart the print scheduler with the following command:

```
/usr/lib/lpsched<return>
```

8.3 GCCS Desktop Printer Concept of Operations

The purpose of this section is to describe the printing capabilities provided by the GCCS Version 2.2

Session Manager (also known as the Desktop). These printing capabilities consist of Network Printing, Remote Printing, and GCCS Development Support.

8.3.1 Network Printing Support. Network Printing Support allows users to send output to printers on their GCCS network regardless of workstation hardware, print server hardware, and printer hardware, within the limitations of the hardware initially identified as supported by the GCCS COE. The following chart describes the combinations of workstation, print server, and printer hardware that are initially supported in the area of networked printing:

CLIENT	PRINT SERVER	PRINTER(S)
SUN Solaris	SUN Solaris	SPARCPrinter II (NEWSPRINT)
		POSTSCRIPT
		Non-POSTSCRIPT (HPCL)
		EPSON Printer
	HP 9.X	POSTSCRIPT
		Non-POSTSCRIPT (HPCL)
		EPSON Printer
HP 9.X	SUN Solaris	SPARCPrinter II (NEWSPRINT)
		POSTSCRIPT
		Non-POSTSCRIPT (HPCL)
		EPSON Printer
	HP 9.X	POSTSCRIPT
		Non-POSTSCRIPT (HPCL)
		EPSON Printer

Network Printing Support consists of support to the System Administrator for printer installation and management and support to

the user for printer selection. System Administrators and users will be provided support for print queue management, and all of these functions will be presented through graphical user interfaces. System Administration printer support will exist as a distinct GCCS application (Printer Administrator) while user print management will be integrated into the GCCS desktop (the User Print Manager function).

8.3.1.1 Printer Administrator. The Printer Administrator function will provide System Administrators the capability to easily manage the functions associated with adding and deleting printers on the GCCS network. Specifically, the following functions will be provided through the printer administrator user interface:

- Install a connected printer on its attached print server.
- Remove an installed printer from its attached print server and all print clients on the network.

Additional functions provided that relate to the management of printer assets on the GCCS network are:

- Query current available printer list and update the client during system reboot or upon administrator request.
- Modify printer characteristics such as description and location.

Queue management functions are similar to functions provided regular users, except that System Administrators are allowed to perform queue management functions across the network and manage jobs that they did not initiate. The queue management tasks supported are:

- Remove any print job from any print queue.
- Move a print job from one print queue to another.
- Start or stop an active print queue.

8.3.1.2 User Print Manager. The User Print Manager enables the user to select the optimal printer for a given print job. The graphical user interface will display a selection list of available printers that includes such details as printer name, print server name, location, description, printer type, and current status. Current status will show how many jobs are currently waiting to be printed on that printer. From this display, the user will select the printer to be used for a given print task. The user will also be enabled to delete jobs that they have initiated from an active print queue.

8.3.2 Remote (Dial-Up) Printing Support. In order to support Army applications that will be reached by modem (through a terminal controller) from remote installations, those applications must be given a method of allowing their output to be directed to a remote printer, either at the dial-up site or potentially at an entirely different remote site. The known constraints on this requirement are that the solution will only be defined for remote print servers that run Windows 3.1 (or potentially Windows NT) or SUN Solaris, and that only character-based applications will be supported remotely.

The solution to this requirement consists of software in three different areas:

- a. The particular configuration of the remote print server
- b. The software that manages the available printer list based on remote logins and logouts (session control)
- c. The software that actually directs the print job to the printer the user selects.

This requirement has one major built-in limitation. The expected maximum throughput is 9600 baud, based on the use of STU-IIIs as modems. This will severely limit the practical size of jobs that can be printed remotely.

8.3.2.1 Remote Print Server Configuration. The remote print server must have the following software, installed in accordance with GCCS installation guidelines: Windows 3.1 (or potentially Windows NT) and Chameleon NFS. Chameleon will allow the remote print server to accept UNIX lpr commands. Only certain types of printers will be supported as remote printers. The following lists the initial configurations supported for remote (dial-up) printer access:

<u>Application Server</u>	<u>Print Server</u>	<u>Printers</u>
SUN Solaris (NEWSPRINT)	SUN Solaris	SPARCPrinter II POSTSCRIPT Non-POSTSCRIPT (HPCL, HPGL) EPSON Printer
SUN Solaris	PC	EPSON Printer

8.3.2.2 Session Control. When a remote user establishes connectivity to the terminal server and logs into an application, the print support software will include the user's local printer on the list of available printers. When the user disconnects from the session, the user's local printer is removed from the available

printer list.

8.3.2.3 Remote Print Software. When a remote user is ready to print from an application on the application server, the user will select from the list of available printers (printers on print servers that are concurrently accessing the terminal server). This is likely to be, but does not have to be, the remote printer at the dial-up users site. The application will send the print command and print file to the associated remote print server for processing.

8.3.3 GCCS Printer Administration User's Guide. The Network Printer Administration Application will allow System Administrators to install, remove and control access to printers on the GCCS network without requiring them to understand the UNIX print commands. All activities revolve around the printer table, so the GCCS System Administrator should view the network printing status in terms of the contents of the printer table. The following sections are step-by-step instructions for performing the major functions of GCCS network printing.

8.3.3.1 Adding A printer to a Print Server

- a. Set up the printer according to the manufacturer's instructions. For Newsprint printers, this includes completing the full Newsprint software and hardware installation. HP printers must be set up to receive serial or parallel input. ASCII and Postscript printers will likely require no special setup.
- b. Plug the printer into the appropriate port on the GCCS system that will be the print server. Serial printers require a 2-3 swap (null modem) if connected to a serial port.
- c. Login as sysadmin on the print server system.
- d. Select the "PRINTER" ICON from the GCCS LAUNCH WINDOW.
- e. When the PRINT MANAGER window appears, select "NEW" from the File pull-down menu.
- f. When the PRINT MANAGER; Create Printer window appears; provide a printername. Names must be 14 characters or less and may not include special characters (dash, underscore, and numerals are allowed).
- g. Provide the printer type. Valid GCCS printer types are HPCL, ASCII, Postscript, or Newsprint.
- h. Provide the port identification.

- i. Provide a printer description. This can be the building, room number, commandname, or whatever will help a user identify this printer. Descriptions can be any length, but for the sake of reasonable-looking printer list displays, it is recommended that they be limited to less than 40 characters.

Selecting the OK or APPLY control button will then create an entry in the GCCS printer table and the UNIX printer table.

The Printer Administration software will make the appropriate system calls to install the printer on the server and then will add an entry to printer table for this printer. Printer

8.3.3.2 Adding Remote Printer

- a. On the PRINT MANAGER window, select New Remote from the File pull-down menu.
- b. When the PRINT MANAGER:Create Non Gccs Printer window appears, enter the PRINTER NAME of the remote printer.
- c. Enter the PRINTER TYPE of the remote printer.
- d. Enter the HOST NAME to which the remote printer is connected.
- e. Enter a DESCRIPTION of the remote printer.
- f. Selecting either OK or APPLY will create a printer in the GCCS printer table as well as an entry in the UNIX printer table.

8.3.3.3 Modifying a GCCS Printer Entry.

- a. On the PRINT MANAGER window, highlight a previously created GCCS printer.
- b. Select Modify from the File pull-down menu.
- c. When the PRINT MANAGER:Modify Printer window appears, make the appropriate changes to the DESCRIPTION field.
- d. Selecting the OK or Apply control buttons will then make the changes to the GCCS printer file.

8.3.3.4 Removing a Printer from the Network

To remove a printer;

- a. Highlight the printer from the list provided in the

PRINTE MANAGER window.

- b. Select 'Delete' from the File pull-down menu.

8.3.3.5 Selecting a GCCS System Default Printer

- a. On the PRINT MANAGER window, highlight the entry that will be the GCCS default printer.
- b. From the File pull-down menu, select Set Default.
- c. When the PRINT MANAGER:Default Printer window appears, select either OK or APPLY. The selected GCCS printer will become the UNIX and GCCS system default printer.

8.3.3.6 Getting Current Printer Status

To get current printer status;

- a. On the PRINT MANAGER window, select the Show Status entry from the Option pull-down menu.
- b. A UNIX lpstat command is then requested, with results displayed in the lower pane of the PRINT MANAGER window.

8.3.3.7 Updating Print Clients on the Network.

The Printer Administration software includes a script that runs on system boot-up that brings the system in synchronization with the printer table. This can also be accomplished by selecting 'Reinitialize Print System' from the Option menu.

8.3.3.8 Terminating the GCCS Printer Admin Manager

When administration of the GSSC printing is complete, select the Exit entry from the file pull-down menu. The application will then terminate.

This same script can be run from the Printer Administration main menu by selecting **Option I: "Update Printers on This Print Client."**

8.3.4 The Current Printer File. Included in the GCCS desktop software is a file that keeps track of the user's current printer. This file is found in the user's home directory and is of the form. `c_p:host_name:session_number` to ensure a unique file name. The current printer file is created each time a user logs into GCCS and remains only as long as the user's current session lasts. During the session, if the user selects a new current printer (using the "File -> Select Printer" option on the GCCS main menu bar) the current printer file will be updated with the new selection.

When a user logs out, two processes occur. First, the contents of the current `.c_p:host_name:session_number` file is copied to a permanent current printer file (called `.c_p` and stored in the user's home directory). Second, the current printer file for that session is deleted.

At login, when the `.c_p:host_name:session_number` file is created, the value in the `.c_p` permanent file (which contains the current printer at the end of this user's last session) is copied into the new current printer file.

If, at login, the `.c_p` file does not contain a currently valid printer (based on the printer table), its value is replaced by the system default printer, which is stored in `/h/data/global/EMDATA/config/.c_p:global`.

If no valid printer exists in any of these files, the `.c_p:host_name:session_number` file will contain the literal `NULL`.

8.3.5 The Printer Table. The printer table is the single system reference that maintains the current status for all GCCS printers on the network. It is located in `/h/data/global/EMDATA/config/printer_table`.

The printer table contains:

- **Printer Entries.** Single line entries, one for each current GCCS printer, that describe the printer's installation status to the printer administration software. The format of each printer entry is:

*Name;Host;Type;Description;Available on Network Flag;Host
O/S;Color Status*

Name -- printer names are limited by UNIX to 14 characters. Printer names cannot contain special characters (except for '-', '_', and '.').

Host -- the system name of the server connected to this printer.

Type -- GCCS supports four broad classes of printers. The valid GCCS printer types are: Postscript, Newsprint, HPCL, and ASCII. Newsprint printers when they are fully installed will be treated as Postscript.

Description -- this is a free-text area, limited (for display purposes) to 64 characters. This field can be used to describe the printer's physical location, its capabilities, which organization it belongs to, or any other information that might be helpful to the user.

Available on the Network -- If this printer is currently available for other clients on the network, this flag should be set to "True." If it is set to "False," only the connected server will be able to print to this printer.

Host O/S -- The Operating System of the connected server host. Valid options are "HP- UX" and "SunOS."

Color Status -- This field contains information that is not being used in the initial delivery of GCCS Printer Administration (all printers are set to "B/W"). When color printing is supported by GCCS, this field will be used to direct color output to the correct printers.

Additionally, each printer is associated with a device, although device information is not stored in the printer table. On HP workstations, available devices are Parallel, Serial A, and Serial B. On SUN workstations, a single port represents both the Serial A and Serial B devices (which one is determined by a switch on the device driver itself).

- Blank Lines. As needed for readability.
- Comment Lines. As needed for readability. Comment lines are lines in the printer table that contain the pound character ('#') anywhere in the line.

Blank lines and comment lines in the printer table are ignored by the Printer Administration software.

One note about editing the printer table -- the addition of a new entry or the modification of a current entry results in the affected entry becoming the last line of the printer table.

8.4 Configuring a System to Print Remotely.

This section discusses how to configure a print client under Solaris and HP-UX operating systems.

8.4.1 Configuring Solaris. (The following can also be done using the Printer Administrator tool.)

- a. Log on to the print client as **root**.
- b. Enter the following command:

```
# lpsystem -t s5 {PRINTSERVER}<return>
      where PRINTSERVER is the name of the print server
```

This response will appear:

{PRINTSERVER} has been added.

Enter the following command:

```
# lpadmin -p {LOCALNAME} -s {PRINTSERVER}!{PRINTERNAME} <return>
where LOCALNAME is the name the printer will be called by the
system.
PRINTSERVER is the host name of the print server.
PRINTERNAME is the name of the printer on the remote print
server.
```

If this will be the default printer, execute the following statement:

```
# lpadmin -d {LOCALNAME}<return>

# accept {LOCALNAME}<return>
  where LOCALNAME is the name the printer will be called
  by the system.

# enable {LOCALNAME}<return>
  where LOCALNAME is the name the printer will be called
  by the system.
```

- c. Check for errors by entering the command:

```
# /bin/lpstat -t<return>
```

8.4.2 Configuring HP-UX

- a. Log on to the print client as **root**.

- b. Enter the following commands:

```
# /usr/lib/lpshut<return>

# /usr/lib/lpadmin -p{LOCALNAME} -m{PRINTMODEL} /
  -v/dev/null -orm{PRINTSERVER} -orp{PRINTERNAME} -ob3 <return>
  where LOCALNAME is the name the printer will be called
  by the system.
  PRINTMODEL is the type of printer.
  PRINTSERVER is the host name of the print server.
  PRINTERNAME is the name of the printer on the remote
  print server.

# /usr/lib/accept {LOCALNAME}<return>
  where LOCALNAME is the name the printer will be called
  by the system.

# /usr/bin/enable {LOCALNAME}<return>
  where LOCALNAME is the name the printer will be called
```

by the system.

/usr/lib/lpsched<return>

SECTION 9. USER ACCOUNT ADMINISTRATION

9.1 Basics about DBUSER 6.0

The database segment DBUSER (Version 6.0.0+) has the capability to create ORACLE User Accounts and granting to the appropriate roles to allow the user to connect to the ORACLE database through any of the 17 following segments:

JOPE\$ (SMDB), RDA, PDR USER, JOPE\$ PDRPT, G\$ORTS, LOGSAFE, JEPES, MEPES, AIRFIELD, RFA DATABASE, TCCESI, NPG, GTN (SMINT) DATABASE, FRAS, GRIS, RPI and EVAC

This segment will not create the GCCS User Accounts. The process to perform that is identified in the following section (**9.2 Adding User Accounts to GCCS**).

The DBUSER segment will also allow for the revoking of specific roles and, if necessary, the revoking of the basic ORACLE User Account. This segment will not delete the GCCS User Accounts created through the process specified in the following section (**9.2 Adding User Accounts to GCCS**).

9.1.1 DBUSER Scripts

The DBUSER segment scripts must be run as either 'root' or 'sysadmin' on the Database Server machine. These routines are located in the /h/DBUSER/progs directory and are called:

```
grant_user  
revoke_user
```

These are Korn Shell scripts that interact with other Korn Shell Scripts and PERL scripts stored in the /h/DBUSER/Scripts directory. The PERL scripts will interface with various SQL scripts that are provided with each segment to actually perform the grants, revokes and any other manipulations that are necessary to properly setup and configure the user accounts. There should be no need for the administrator to directly call any routine other than the two listed above.

9.1.2 Log Files

The various SQL scripts that grant and revoke the privileges, and in a few cases create tables, remove tables, etc.; will generate numerous log files in the /tmp directory. These are generally named in an obvious fashion. But if the administrator desires these to be displayed a bit more clearly, when invoking either of the two scripts mentioned above simply add the argument '-v' at the end. The spool log file names will be displayed after each grant or revoke is performed.

When using the MULTIPLE user mode, explained below, only the last log

files are saved since as each user is processed the log files from the prior user will be overwritten with the new user log file activities.

9.1.3 DBUSER Interface

The DBUSER interface is geared towards a line based interface that prompts the user with questions about which roles to grant or revoke. There is an occasional need to request a password from the user and verify that it is acceptable. When this happens an X Term window will be displayed prompting for the desired password. The questions that are asked are phrased to be responded to with a YES or a NO, and should be limited to a 'Y' (for YES) or a 'N' (for NO).

9.2 Adding User Accounts to GCCS

It is recommended that user accounts be established after all software is loaded on all platforms and NIS+ is initialized.

Two administrative accounts are delivered with the software:

secman - used to add user accounts or profiles.

sysadmin - used to perform system administrator functions, such as installation of new segments.

The installation team will assist the Site Administrator in creating an account for the System Administrator (to be used for user account maintenance) and a basic user account. The following steps must be followed.

9.2.1 Creating User Accounts (Performed at the EM Server's Console.)

- a. Log in as **secman**, with proper password.
- b. Select **Prefs** from the menu bar. Select **Change Profile** from the menu. Click the **Next** or **Prev** buttons until **SYSADMIN** is displayed in the **Position:** field. Click the **OK** button.
- c. Double click the **Security** icon. The **run_security** window displays. Enter the secman's password at the Password: prompt. The **Security Manager** window appears.
- d. Select **File** from the menu bar. Select **Create Account** from the menu. The **SECURITY MANAGER: Create Accounts** window appears.
- e. Enter the **USER ID:** 8 characters or less, starting with an alphabetic character (a-z), and containing only alphanumeric characters and the underscore (_).
- f. Enter the **USER NAME:** (Essentially an administrative comment field. Recommended: section; POC Information, including location and telephone number. Example: ccj6_doc MAJ John Doe 8-6580.)

NOTE: Do not use commas or other special characters. Use only letters and numerals.

- g. The **USER #** field is filled in by the utility. (This is the UID and it is the last used value plus 1. This number may be edited to re-use old UID #s that have been deleted).
- h. Enter the **PASSWORD:** (This will be the user's login password).
- i. Enter the **SYBASE SYS ADMIN USERNAME:** (sa).
- j. Enter the **SYBASE SYS ADMIN PASSWORD:** (See Section 11.1).
- k. Click the button for the **DEFAULT GROUP:** field. Select from: **admin** (for an administrator account) or **gccs** (for a user account). Click the **Apply** button.
- l. Click the button for the **OPTIONAL GROUP:** field. Select from: **admin** (for an administrator account) or **gccs** (for a user account). Click the **Apply** button.
- m. Click the button for the **Acct_groups** field. Select from: **root**, **Security Admin**, **System Admin**, or **GCCS Operator** (for a user account). Click the **Apply** button.
- n. Click the button for the **Role** field. Select from: **SSO Default** (user account management and security), **SA Default** (system administration, which is primarily used for installing new software segments), or **GCCS Default** (for a user account). Click the **Apply** button.
- o. When all fields are successfully completed, click the **OK** button on the SECURITY MANAGER: Create Accounts window.
- p. Select **File** from the menu bar. Select **Exit** from the menu. Click **OK** to the Exit? question.

9.2.2 Customizing Profiles. After the System Administrator has registered the new user, a user profile must be assigned for the user.

- a. Log in as **secman**, with proper password.
- b. Select **Prefs** from the menu bar. Select **Change Profile** from the menu. Click the **Next** or **Prev** buttons until SYSADMIN is displayed in the Position: field. Click the **OK** button.
- c. Double click the **Profile** icon. The Profile Manager window appears.

- d. Select **File** from the menu bar. Select **Add New User Profile** from the menu. The PROFILE MANAGER: Add New User Profile window appears.
- e. Click the button for the **User ID:** field. Select appropriate user from the registered users display.
- f. Click the button for the **Project:** field. Select appropriate project from the display.
- g. Click the button for the **Position:** field. Select from: GCCSUSER or SYSADMIN in the position display. (This selection is tied to the user's launch window icon selections.)

NOTE: These first three fields of the window are mandatory for user profile creation. The others deal with the organizational structure of the site. They include Directorate, Division, Branch, Section, and Cell.

- h. Click on the **OK** or **Apply** button. Select **File** from the menu bar and **Exit** from the menu.

9.3 Executing the 'grant_user' DBUSER Script

The grant_user script will perform some basic setup options:

- a. Determine the DISPLAY that will be used for the secondary windowing prompting by checking the setting of the DISPLAY environment variable. If it is NULL it will request the DISPLAY to use. This allows the administrator to run the script on a machine other than the DBSERVER, but remotely connected through an X Windows terminal session. If done remotely the local machine should have 'xhost +' enabled to allow the X Windows DISPLAY to be shown on the local machine.

- b. The password for the oradba account will be requested through a secondary xterm window displayed in yellow. This window will verify the password provided. A correct password must be entered before the script will allow further use. If the oradba password is set to be INTERNAL then simply entering a NULL value (hitting RETURN) will verify that as a valid password.

When these two housekeeping tasks are accomplished the user is requested which of the two modes of operation to use 'S'ingle or 'M'ultiple User. To exit the script enter 'Q'uit at this prompt.

9.3.1 Working in SINGLE USER Mode

By selecting the 'S' option the administrator will be prompted to provide a user name that needs to be manipulated. This user name should be an existing GCCS account that was created using the procedure described in

section X.2. It should consist of one (1) to eight (8) characters beginning with an alphabetic (A-Z) followed by alphanumeric (A-Z, 0-9) or the underscore (_) character. When creating a UNIX account the case (upper or lower) is important, but within ORACLE any lowercase characters are converted to uppercase. The grant_user script will translate any names provided to uppercase.

The grant_user script will determine if the user name provided currently has ORACLE CONNECT privileges. If it does not have such privileges the administrator will be prompted whether the ORACLE account should be created. Answering this question with 'Y' will grant CONNECT privileges to the account with appropriate SQL responses displayed. Answering this question with a 'N' will return the script to the MODE Prompt.

If the user name already has CONNECT privileges, or the CONNECT privileges are granted the grant_user script will determine what other ORACLE roles if any are currently granted to the user. This set of ORACLE roles is used in the following series of questions.

For each Database Segment currently installed on the database server there is one, or more ORACLE roles that need to be granted for a user to access that database segment. The primary ORACLE role for the segment is compared against the list of ORACLE Roles determined in the following step. If the user already has that role no action will be taken. If, however, the user does not have the primary ORACLE role for the segment then the administrator will be prompted whether the user should be granted that role or not. The answer for each question is stored for bulk processing in the next step.

When all of the installed database segments have been checked and queried against the administrator will have displayed all of the role(s) that have been chosen to be granted. The administrator will then be prompted whether this list is correct and these roles should be granted to this user. If the answer is 'N' the script will return to the MODE Prompt. If the answer is 'Y' then the next step is performed.

For each role to be granted the set of scripts provided with the database segments to grant the role, create the tables, create the synonyms, etc. will be run in the sequence necessary to properly configure the ORACLE user for accessing the specified database segment via the corresponding client segment. Most of these scripts are very straightforward and simply grant the specified role to the specified user. But some are much more elaborate and involved. Success or failure to grant the role will be displayed after each script is processed.

9.3.2 Working in MULTIPLE USER Mode

By selecting the 'M' option the administrator will be prompted to provide a sequence of user names that needs to be manipulated. These user names should be existing GCCS accounts that were created using the procedure described in section X.2. Each name should consist of one (1) to eight

(8) characters beginning with an alphabetic (A-Z) followed by alphanumeric (A-Z, 0-9) or the underscore (_) character. When creating a UNIX account the case (upper or lower) is important, but within ORACLE any lowercase characters are converted to uppercase. The grant_user script will translate any names provided to uppercase. Each name should be followed by a <return> to separate them. After entering the last name enter a single period (.) character followed by a <return>.

For each user name entered the grant_user script will perform the following steps:

- a. Determine if the user name provided currently has ORACLE CONNECT privileges. If it does not have such privileges the script will grant CONNECT privileges to the account with appropriate SQL responses displayed.
- b. All of the ORACLE roles currently granted to the user will be determined and stored for use in step (e).
- c. For the first user only the set of ORACLE roles to be granted will be determined. For each Database Segment currently installed on the database server there is one, or more ORACLE roles that need to be granted for a user to access that database segment. The administrator is queried for each role whether it should be granted to this set of users. These answers are stored for use in step (e).
- d. After the administrator has responded to each role question, the list of roles to be granted is displayed and the administrator is asked to confirm the choice. If the answer is 'Y'es then the roles will be granted as stated below. If the answer is 'N'o then the process will be cancelled and the routine will return to the MODE prompt.
- e. For each role chosen to be granted a test is made to see if the user already has that role. This is done by comparing the list saved from step (b) and the list from step (c). If the user does not have the role then step (f) is performed.
- f. The role to be granted has a set of scripts provided with the database segments to grant the role, create the tables, create the synonyms, etc. This set of scripts will be run in the sequence necessary to properly configure the ORACLE user for accessing the specified database segment via the corresponding client segment. Most of these scripts are very straight forward and simply grant the specified role to the specified user. But some are much more elaborate and involved. Success or failure to grant the role will be displayed after each script is processed.

As mentioned in step (c) only on the first user will there be a query for which roles to grant. This list once built will be used for each of the other users so that when processing is completed all of the users will have the same set of new roles.

9.4 Executing the 'revoke_user' DBUSER Script

The revoke_user script will perform some basic setup options:

a. Determine the DISPLAY that will be used for the secondary windowing prompting by checking the setting of the DISPLAY environment variable. If it is NULL it will request the DISPLAY to use. This allows the administrator to run the script on a machine other than the DBSERVER, but remotely connected through an X Windows terminal session. If done remotely the local machine should have 'xhost +' enabled to allow the X Windows DISPLAY to be shown on the local machine.

b. The password for the oradba account will be requested through a secondary xterm window displayed in yellow. This window will verify the password provided. A correct password must be entered before the script will allow further use. If the oradba password is set to be INTERNAL then simply entering a NULL value (hitting RETURN) will verify that as a valid password.

When these two housekeeping tasks are accomplished the user is requested which of the two modes of operation to use 'S'single or 'M'multiple User. To exit the script enter 'Q'uit at this prompt.

9.4.1 Working in SINGLE USER Mode

By selecting the 'S' option the administrator will be prompted to provide a user name that needs to be manipulated. This user name should be an existing GCCS account that was created using the procedure described in section X.2. It should consist of one (1) to eight (8) characters beginning with an alphabetic (A-Z) followed by alphanumeric (A-Z, 0-9) or the underscore (_) character. When creating a UNIX account the case (upper or lower) is important, but within ORACLE any lowercase characters are converted to uppercase. The revoke_user script will translate any names provided to uppercase.

The revoke_user script will determine if the user name provided currently has ORACLE CONNECT privileges. If it does not have such privileges a message will be displayed and the script will return to the MODE prompt.

If the user name already has CONNECT privileges, the revoke_user script will determine what other ORACLE roles are currently granted to the user, if any. This set of ORACLE roles is used in the following series of questions.

The first question will be if all of the roles including the CONNECT privilege should be revoked from the specified user. If the answer is 'Y'es then the 'revoke_user' script will assume that ALL of the roles should be revoked as well and not bother to prompt for them. If the answer is 'N'o then the questions below are asked.

For each Database Segment currently installed on the database server

there is one, or more ORACLE roles that need to be revoked from the user. The primary ORACLE role for the segment is compared against the list of ORACLE Roles determined in the following step. If the user already has that role the administrator will be prompted whether that role should be revoked or not. If, however, the user does not have that role no action will be taken. For each question the answer is stored for bulk processing in the next step.

When all of the installed database segments have been checked and queried against, the administrator will have displayed all of the role(s) that have been chosen to be revoked. The administrator will then be prompted whether this list is correct and these roles should be revoked from this user. If the answer is 'N' the script will return to the MODE Prompt. If the answer is 'Y' then the next step is performed.

For each role to be revoked the set of scripts provided with the database segments to revoke the role, drop the tables, drop the synonyms, etc. will be run in the sequence necessary to properly revoke access from the ORACLE user from the specified database segment via the corresponding client segment. Most of these scripts are very straightforward and simply revoke the specified role to the specified user. But some are much more elaborate and involved. Success or failure to revoke the role will be displayed after each script is processed.

If the administrator chose to drop the CONNECT privilege then the sql script stored in \$ORACLE_HOME to drop the user entirely shall be run.

9.4.2 Working in MULTIPLE USER Mode

By selecting the 'M' option the administrator will be prompted to provide a sequence of user names that needs to be manipulated. These user names should be existing GCCS accounts that were created using the procedure described in section X.2. Each name should consist of one (1) to eight (8) characters beginning with an alphabetic (A-Z) followed by alphanumeric (A-Z, 0-9) or the underscore (_) character. When creating a UNIX account the case (upper or lower) is important, but within ORACLE any lowercase characters are converted to uppercase. The grant_user script will translate any names provided to uppercase. Each name should be followed by a <return> to separate them. After entering the last name enter a single period (.) character followed by a <return>.

For each user name entered the revoke_user script will perform the following steps:

- a. Determine if the user name provided currently has ORACLE CONNECT privileges. If it does not have such privileges the script skip this user and proceed with the next user at this step.
- b. All of the ORACLE roles currently granted to the user will be determined and stored for use in step (f).

- c. For the first user, who has connect privileges, the administrator will be queried if ALL of the ORACLE roles, including the CONNECT PRIVILEGE should be revoked. If this answer is 'Y'es then all roles granted shall be revoked, including the CONNECT PRIVILEGE and step (d) below is skipped. If this answer is 'N'o then step (d) is performed.
- d. The set of ORACLE roles to be revoked will be determined. For each Database Segment currently installed on the database server there is one, or more ORACLE roles that need to be revoked from the user. The administrator is queried for each role whether it should be revoked from this set of users. These answers are stored for use in step (f).
- e. After the administrator has responded to each role question, the list of roles to be revoked is displayed and the administrator is asked to confirm the choice. If the answer is 'Y'es then the roles will be revoked as stated below. If the answer is 'N'o then the process will be cancelled and the routine will return to the MODE prompt.
- f. For each role chosen to be revoked a test is made to see if the user already has that role. This is done by comparing the list saved from step (b) and the list from step (d). If the user does have the role then step (g) is performed.
- g. The role to be revoked has a set of scripts provided with the database segments to revoke the role, drop the tables, drop the synonyms, etc. This set of scripts will be run in the sequence necessary to properly revoke access from the ORACLE user from the specified database segment via the corresponding client segment. Most of these scripts are very straightforward and simply revoke the specified role to the specified user. But some are much more elaborate and involved. Success or failure to revoke the role will be displayed after each script is processed.
- h. If the administrator in step (c) chose to drop the CONNECT privilege then the sql script stored in \$ORACLE_HOME to drop the user entirely shall be run.

As mentioned in steps (c) and (d) only on the first user will there be a query for which roles to revoke. This list once built will be used for each of the other users so that when processing is completed all of the users will have the same set of roles revoked.

9.5 Notes Relating to specific GCCS Segments

This section details some rather specific information concerning each of the current Database Segments that the DBUSER segment interfaces with. The information contained herein is technical information that is useful

in understanding the log files generated and how to correct problems should they arise.

9.5.1 JOPES

The JOPES Database Segment is referred to as SMDB. The primary role name is 'SMDB_USER'. The secondary role name is 'SMDB_REF_FILE'. This secondary role is only present when the SMDB Patch 15 Segment is installed. To grant the roles necessary to access the SMDB segment, two (2) SQL scripts are run. The first is stored in the DBUSER Segment, the second is generated dynamically from the first and is stored temporarily in the /tmp directory. When revoking the JOPES Segment from a user, the user needs to have either the 'SMDB_USER' role or the 'SMDB_REF_FILE' role for the revoke script to be executed. This revoke will run two (2) SQL scripts, the first stored in the DBUSER Segment, the second is generated dynamically from the first and is stored temporarily in the /tmp directory.

9.5.2 RDA

The RDA Database Segment is referred to as RDASRV. The role name is 'RDAUSER'. To grant the role necessary to access the RDASRV Segment, one (1) SQL script stored in the RDASRV Segment is run. To revoke the role one (1) SQL script stored in the RDASRV Segment is run.

9.5.3 PDR USER

The PDR USER Database Segment is referred to as PDRSRV. The role name is 'PRE_DEFINED_REPORTS_USER'. To grant the role and create the necessary database objects there are four (4) SQL scripts stored in the PDRSRV Segment to run. To revoke the role and drop the database objects there are four (4) SQL scripts stored in the PDRSRV Segment to run.

9.5.4 JOPES PDRPT

The JOPES PDRPT Database Segment is referred to as JOPES_ORA_PDRPT. The role name is 'JPDRPT_ROLE'. To grant the role there is one (1) SQL script stored in the JOPES PDRPT Segment to run. To revoke the role there is one (1) SQL Script stored in the JOPES PDRPRT Segment to run.

9.5.5 GSORTS

The GSORTS Database Segment is referred to as GORA. The role name is 'GSORTS_ROLE'. To grant the role there is one (1) SQL script stored in the GSORTS Segment to run. To revoke the role there is one (1) SQL Script stored in the GSORTS Segment to run.

9.5.6 LOGSAFE

The LOGSAFE Database Segment is referred to as OLSAFE. The role name is 'LOGSAFE_USER'. To grant the role there are three (3) SQL scripts stored

in the OLSAFE Segment to run. To revoke the role there are five (5) SQL Scripts needed to be run. Four (4) of the scripts are stored in the OLSAFE Segment. The last is generated and is stored in the / tmp directory.

9.5.7 JEPES

The JEPES Database Segment is referred to as OJEPES. The role name is 'JEPES_USER'. To grant the role the administrator must provide the table_master password. When this has been successfully retrieved, one (1) SQL Script stored in the OJEPES Segment will be run. To revoke the role there are two (2) SQL Scripts stored in the OJEPES Segment to run.

9.5.8 MEPES

The MEPES Database Segment is referred to as MEPESDB. The role name is 'MEPES_USER'. To grant the role there is one (1) SQL script stored in MEPESDB Segment to run. To revoke the role there is one (1) SQL Script stored in the MEPESDB Segment to run.

9.5.9 AIRFIELD

The AIRFIELD Database Segment is referred to as AIRFDB. The role name is 'AIRFIELD_ROLE'. To grant the role there is one (1) SQL script stored in the AIRFDB Segment to run. To revoke the role there is one (1) SQL Script stored in the AIRFDB Segment to run.

9.5.10 RFA DATABASE

The RFA Database Segment is referred to as RFADB. The role name is 'RFA_USER'. To grant the role the administrator must provide the table_master password and the RFA password. When these have been successfully retrieved, seven (7) SQL Scripts need to be run. Four (4) of the seven (7) are stored in the RFADB Segment. The other three (3) are generated by the first four Scripts and are stored in the / tmp directory. To revoke the role the administrator must provide the RFA password. When this has been successfully retrieved, six (6) SQL Scripts need to be run. Three (3) of the six (6) are stored in the RFADB Segment. The other three (3) are generated by the first three Scripts and are stored in the / tmp directory

9.5.11 TCCESI

The TCCESI Database Segment is referred to as ESISRV. The role name is 'TCCESI'. To grant the role there is one (1) SQL script stored in the ESISRV Segment to run. To revoke the role there is one (1) SQL Script stored in the ESISRV Segment to run.

9.5.12 NPG

The NPG Database Segment is referred to as NPGDB. The role name is

'NPG_USER'. To grant the role there is one (1) SQL script stored in the NPGDB Segment to run. To revoke the role there is one (1) SQL Script stored in the NPGDB Segment to run.

9.5.13 GTN (SMINT) DATABASE

The GTNSMINT Database Segment is referred to as SMIDB. The role name is 'GTNSMINT_ROLE'. To grant the role there is one (1) SQL script stored in the GTNSMINT Segment to run. To revoke the role there is one (1) SQL Script stored in the GTNSMINT Segment to run.

9.5.14 FRAS

The FRAS Database Segment is referred to as FRASDB. The role name is 'FRAS_ROLE'. To grant the role there is one (1) SQL script stored in the FRASDB Segment to run. To revoke the role there is one (1) SQL Script stored in the FRASDB Segment to run.

9.5.15 GRIS

The GRIS Database Segment is referred to as GRISDB. The role name is 'GRIS_ROLE'. To grant the role there is one (1) SQL script stored in GRISDB Segment to run. To revoke the role there is one (1) SQL Script stored in the GRISDB Segment to run.

9.5.16 RPI

The RPI Database Segment is referred to as RPIDB. The role name is 'RPI_USER'. To grant the role there is one (1) SQL script stored in the RPIDB Segment to run. To revoke the role there is one (1) SQL Script stored in the RPIDB Segment to run.

9.5.17 EVAC

The EVAC Database Segment is referred to as EVACDB. The role name is 'EVAC_ROLE'. To grant the role there is one (1) SQL script stored in the EVACDB Segment to run. To revoke the role there is one (1) SQL Script stored in the EVACDB Segment to run.

SECTION 10. SOFTWARE LICENSE ADMINISTRATION

10.1 Applix License Setup Procedures

To use Applix the license must be installed. Execute the following to obtain your License Key:

- a. Log in as **root**, then execute the following:

```
# cd /h/COTS/APPLIX/axdata <return>
```

```
# ./axhostid <return>
```

NOTE: The system will identify the site's License Key. Contact the GMC Hotline at (703) 695-0671 or DSN 225-0671 and provide the License Key and POC (NAME, TEL, FAX). DISA will notify Applix, obtain the licensing information for the site, and FAX it to the site POC, usually within 24 hours.

- b. Execute the following:

```
# cd /h/COTS/APPLIX/axdata <return>
```

- c. Two license files will appear: *axlicensedemo*, *alxicensdat*

1. The following is an example of the information that will be executed when *axlicensedemo* is opened:

```
FEATURE *wgm none 3.000 1-dec-95 0 8B4C1F6D076650F27859 "" DEMO
FEATURE *sps none 3.000 1-dec-95 0 4B7C4F4D381F2609F469 "" DEMO
FEATURE *mbx none 3.000 1-dec-95 0 7BDC2F3D48AF4E68BAB1 "" DEMO
FEATURE *fwp none 3.000 1-dec-95 0 5B4C3FCD88E32B76C59F "" DEMO
FEATURE *fpp none 3.000 1-dec-95 0 4B7C4FED95F02D79C59F "" DEMO
FEATURE *fgp none 3.000 1-dec-95 0 8B4C1FCD58B34B66C59F "" DEMO
FEATURE *dat none 3.000 1-dec-95 0 7BAC2F6D54BF4D6AC7A7 "" DEMO
FEATURE *opn none 3.000 1-dec-95 0 4B7C2FBD8CEBF81AC019 "" DEMO
FEATURE *rts none 3.000 1-dec-95 0 5B3C3F5D2D1027FEF16F "" DEMO
```

2. The following is an example of the information that will be executed when *axlicensdat* is opened:

```
FEATURE *sps none 3.000 1-dec-95 0 4B7C4F4D381F2609F469 "" DEMO
FEATURE *mbx none 3.000 1-dec-95 0 7BDC2F3D48AF4E68BAB1 "" DEMO
FEATURE *fwp none 3.000 1-dec-95 0 5B4C3FCD88E32B76C59F "" DEMO
FEATURE *fpp none 3.000 1-dec-95 0 4B7C4FED95F02D79C59F "" DEMO
FEATURE *fgp none 3.000 1-dec-95 0 8B4C1FCD58B34B66C59F "" DEMO
FEATURE *dat none 3.000 1-dec-95 0 7BAC2F6D54BF4D6AC7A7 "" DEMO
FEATURE *opn none 3.000 1-dec-95 0 4B7C2FBD8CEBF81AC019 "" DEMO
FEATURE *rts none 3.000 1-dec-95 0 5B3C3F5D2D1027FEF16F "" DEMO
```

- d. Execute the following:

 # cd /h/COTS/APPLIX
- e. Type **applix**.
- f. From the Applix utility menu, select **LICENSEGENERATOR**.
- g. Using the license information sheet provided by DISA, enter all information, tabbing between fields. All entries are in upper case.
- h. After entering all data, choose **OK**.
- i. To ensure that the APPLIX license manager comes up when the system is re-booted, execute the following:

```
# cd /etc/rc3.d
```

```
# vi S4Sapplix
```

Add the following lines:

```
./h/COTS/APPLIX/axdata/axlnmgrd -c\
```

```
./h/COTS/APPLIX/axdata/axlicenseda > /tmp/axnlmlog &
```

10.2 JDISS License Setup Procedures

The JDISS will not run if the site has not obtained a license. Contact the GMC at (703-695-0671/ DSN225-0671) to find out how to obtain a license.

10.2.1 Client/Server Relationship. For JDISS to run properly, the JDISS license must be on the host designated "lmserver." The JDISS client segment must be loaded on a host that can reach the lmserver, i.e., the `/etc/inet/hosts` file must have the IP address and "lmserver" of the host that has the JDISS server segment loaded.

10.2.2 License File Procedures for JDISS Version 2.0.3

NOTE: The license file is called *license.dat* and is in ASCII text format. Most of the file contents should not be changed. The server host ID cannot be changed without getting a new license file from the JDISS PMO. In the DAEMON line, the path to the daemon can be modified. If any other changes are made, it will invalidate the license, and the application will not be found.

If a site has a license, or if the host machine is a client of another host that has a network license then, to install the JDISS license file

for JDISS v2.0.3:

- a. Copy the *license.dat* file the site received to */h/JDISS/etc* as follows:

```
# cp license.dat /h/JDISS/etc Re-boot the machine.
```

Installation is complete.

10.2.3 Procedures for Machines Currently Running Older Version That Upgrade v2.0.3.

Before upgrading to JDISS V2.0.3, save the */h/JDISS/etc/license.dat* files to another directory, so the files will not be deleted.

- a. After installing V2.0.3, copy the saved *license* to the JDISS directory as follows:

```
# cp license.dat/h/JDISS/etc/license.dat
```

- b. Re-boot the machine. Installation is complete.

Troubleshooting of JDISS for troubleshooting procedures see JDISS Installation Manual dated, 7 November 1996 or JDISS System Administration Manual dated, 7 November 1996.

10.3 NeWSprint License Setup Procedures

10.3.1 NeWSprint Version 2.0 Setup Procedure. To install the font license, the site must have a font password. Also, if the site has a Postscript printer, such as a Laserwriter, it does not need a font license.

10.3.1.1 Acquiring a Font Password. A font password can be acquired by calling 1-800-USA-4SUN and supplying the following information.

- Host ID of the system to which the printer is attached.
- Serial number of the NeWSprint software. The serial number is printed around the inside hole of the NeWSprint CD.
- The NeWSprint "right to use" number, listed on the face of the licensing agreement.

After acquiring the password, install the software, and set up the license that was provided by SUN Systems.

10.3.2 Upgrading a License for NeWSprint V2.0 to V.2.1. If a site is using NeWSprint 2.0, the original password is still valid for NeWSprint 2.1. To check the fonts, execute the following:

```
# cd /var/spool/license/fontlicense
```

Example (a number should appear that is similar to this font license: .65000934):

```
# cat /var/spool/licenses/fontlicenses.65000943
```

NOTE: Host ID and font password will be displayed.

NOTE: The installing license procedures are the same as in Section 2.0, "Setup Procedures."

10.3.3 NeWSprint Version 2.5 License Setup Procedures

- a. Call SUN Systems at 1-800-USA-4SUN during the hours of 0800 to 1700 Monday through Friday to obtain font password. You must have the same information as listed in Section 2.0.
- b. To view the host ID and font password, execute the following:

```
# /opt/NeWSprint/bin/hostid
```


SECTION 11. SPARCSTORAGE ARRAY ADMINISTRATION

11.1 Overview

This section provides a description of the steps that are performed to remove and install disk drives in SPARCstorage arrays in typical GCCS environments. The steps in this section have been refined and condensed; however, they are intended to be in total compliance with the procedures described in the *SPARCstorage Array Configuration Guide*. If any discrepancies exist between this document and the *SPARCstorage Array Configuration Guide*, the *SPARCstorage Array Configuration Guide* takes precedence.

Before performing functions to modify the configuration administrative personnel should be familiar with the various types of SPARCstorage array configurations provided with the Volume Manager (VM), the graphical representation of VM objects (disks, disk groups, subdisks, plexes, volumes), standard GCCS configuration guidelines, and any site-specific implementations.

The SPARCstorage arrays are normally configured as part of the process to build a new GCCS operating environment or to upgrade an existing one. Disk partition and mapping guidelines for the various GCCS SUN SPARCserver and client platforms are provided in the *GCCS Implementation Procedures* document.

11.2 GCCS Configuration Considerations

When a partition from a physical disk is placed under VM control, a VM disk is assigned to the partition and is accessed via a disk media name (e.g., *oracle17*). The assigned VM disk also becomes a part of a disk group (e.g., *oracledg*), a collection of VM disks that have something in common. A VM disk can be divided into one or more subdisks. Subdisk names are derived from their respective VM disk media name (e.g., *oracle17-01*).

VM uses subdisks to build virtual devices, which are called "plexes." A plex consists of one or more subdisks that can be located on one or more physical disks. Plex names are derived from their associated volume name (e.g., *vol02-01* indicates the first plex of the second volume, *vol02*). A volume can consist of one to eight plexes. VM default naming conventions are used to uniquely label volumes (e.g., *vol02*).

In an array-only hardware environment (no internal or other external disk devices), the standard GCCS VM installation functions will designate the last disk device in the first array for swap use. This disk, along with any other disks that are not under VM control, will be presented with a "failed" status in the VM GUI displays and in output

produced from executing the VM command line interface (CLI) *vxdisk list* command.

VM disk striping and mirroring techniques are used in the standard GCCS disk configuration functions for certain file systems to optimize system performance and provide enhanced data protection. This process builds VM volumes by sequentially selecting the first available physical disk (logical subdisk) associated with each target number. This process is repeated until a sufficient number of disks are obtained to build a volume of desired size and structure.

Additionally, at least one disk contained on each array is designated as a Hot Spare (HS) disk. Hot-sparing, a VM configuration option, is used to automatically rebuild mirrored data when a disk fails. When a disk fails in a disk group with an HS disk, the failed physical disk disappears from the disk group view and the HS disk assumes the characteristics of the failed disk, including its name and subdisks. HS disks can only be used to replace disks in the disk group to which they have been assigned. If no disk is designated as an HS device, data on a disk that fails is lost.

Consequently, in building striped, mirrored volumes using two 18GB SPARCstorage arrays and designating an HS disk on each unit, the GCCS VM installation process produces a configuration in the following manner (as depicted in the sample output from a *vxdisk list* command):

DEVICE	TYPE	DISK	GROUP	STATUS
c3t0d0s2	sliced	oracle01	oracledg	online
c3t0d1s2	sliced	oracle07	oracledg	online
c3t0d2s2	sliced	oracle13	oracledg	online
c3t1d0s2	sliced	oracle08	oracledg	online
c3t1d2s2	sliced	oracle14	oracledg	online
c3t2d0s2	sliced	oracle03	oracledg	online
c3t2d1s2	sliced	oracle09	oracledg	online
c3t2d2s2	sliced	oracle15	oracledg	online
c3t3d0s2	sliced	oracle04	oracledg	online
c3t3d1s2	sliced	oracle10	oracledg	online
c3t3d2s2	sliced	oracle16	oracledg	online
c3t4d0s2	sliced	oracle05	oracledg	online
c3t4d1s2	sliced	oracle11	oracledg	online
c3t4d2s2	sliced	oracle17	oracledg	online
c3t5d0s2	sliced	oracle06	oracledg	online
c3t5d1s2	sliced	oracle12	oracledg	online
c3t5d2s2	sliced	spare01	oracledg	online spare
c4t0d0s2	sliced	mirror01	oracledg	online
c4t0d1s2	sliced	mirror07	oracledg	online
c4t0d2s2	sliced	mirror13	oracledg	online
c4t1d0s2	sliced	mirror02	oracledg	online
c4t1d1s2	sliced	mirror08	oracledg	online

c4t1d2s2	sliced	mirror14	oracledg	online
c4t2d0s2	sliced	mirror03	oracledg	online
c4t2d1s2	sliced	mirror09	oracledg	online
c4t2d2s2	sliced	mirror15	oracledg	online
c4t3d0s2	sliced	mirror04	oracledg	online
c4t3d1s2	sliced	mirror10	oracledg	online
c4t3d2s2	sliced	mirror16	oracledg	online
c4t4d0s2	sliced	mirror05	oracledg	online
c4t4d1s2	sliced	mirror11	oracledg	online
c4t4d2s2	sliced	mirror17	oracledg	online
c4t5d0s2	sliced	mirror06	oracledg	online
c4t5d1s2	sliced	mirror12	oracledg	online
c4t5d2s2	sliced	spare02	oracledg	online spare

Where *c#* denotes the controller number associated with the array units, *t#* indicates the target number (0-5) within the referenced array, *d#* indicates the disk number (0-4) associated with each respective target number, and *s2* indicates that the full disk is being used as a subdisk partition.

The order of the disk names *oracle##* and *mirror##* indicates that the first available disk was selected from the first target number, followed by the selection of the next available disk on the next target number, and so on, until all required disks were selected. HS disks have been named *spare01* and *spare02*. In practice, this list would also include any additional disks that are present on the platform but are not under VM control (with an error status).

11.3 Identifying a Failed Disk

The key aspect of disk replacement involving a SPARCstorage Array unit is identifying the proper disk device to remove or replace.

11.3.1 Command Line Interface Techniques. The VM CLI can be used to produce a list of available disk devices and their related status. The list will indicate which VM controlled disks are in an error status. Note that in the standard GCCS configuration, the designated swap disk and other disks not under VM control will also be listed with an error status. The following steps are performed to identify failed disk devices using the VM CLI:

- a. Log in as **root**.
- b. Produce a list of available disk devices:


```
# vxdisk list | more
```
- c. Review the generated output to identify devices that have an error status, situations where an HS device has kicked in, and situations where the volume components do not comply

with the standard GCCS configuration techniques. For example, considering the previous `vxdisk` list output for a scenario containing a failed disk:

DEVICE	TYPE	DISK	GROUP	STATUS
c3t0d0s2	sliced	oracle01	oracledg	online
c3t0d1s2	sliced	oracle07	oracledg	online
c3t0d2s2	sliced	oracle13	oracledg	online
c3t1d0s2	sliced	oracle02	oracledg	online
c3t1d1s2	sliced	oracle08	oracledg	online
c3t1d2s2	sliced	oracle14	oracledg	online
c3t2d0s2	sliced	oracle03	oracledg	online
c3t2d1s2	sliced	oracle09	oracledg	online
c3t2d2s2	sliced	oracle15	oracledg	online
c3t3d0s2	sliced	oracle04	oracledg	online
c3t3d1s2	sliced	-	-	error
c3t3d2s2	sliced	oracle16	oracledg	online
c3t4d0s2	sliced	oracle05	oracledg	online
c3t4d1s2	sliced	oracle11	oracledg	online
c3t4d2s2	sliced	oracle17	oracledg	online
c3t5d0s2	sliced	oracle06	oracledg	online
c3t5d1s2	sliced	oracle12	oracledg	online
c3t5d2s2	sliced	oracle10	oracledg	online
c4t0d0s2	sliced	mirror01	oracledg	online
c4t0d1s2	sliced	mirror07	oracledg	online
c4t0d2s2	sliced	mirror13	oracledg	online
c4t1d0s2	sliced	mirror02	oracledg	online
c4t1d1s2	sliced	mirror08	oracledg	online
c4t1d2s2	sliced	mirror14	oracledg	online
c4t2d0s2	sliced	mirror03	oracledg	online
c4t2d1s2	sliced	mirror09	oracledg	online
c4t2d2s2	sliced	mirror15	oracledg	online
c4t3d0s2	sliced	mirror04	oracledg	online
c4t3d1s2	sliced	mirror10	oracledg	online
c4t3d2s2	sliced	mirror16	oracledg	online
c4t4d0s2	sliced	mirror05	oracledg	online
c4t4d1s2	sliced	mirror17	oracledg	online
c4t5d0s2	sliced	mirror06	oracledg	online
c4t5d1s2	sliced	mirror12	oracledg	online
c4t5d2s2	sliced	spare02	oracledg	online spare

Examination of the output shows device `c3t3d1s2` with an "error" status indicating that the device has failed. Additionally, it can be determined that device `c3t5d2s2`, an HS device, has kicked in and is now regarded as disk `oracle10`, and whose status no longer indicates that it is spare disk.

- d. Record and save the failed disk name, along with its actual and normal device addresses (if the HS has kicked in) for reference during configuration restoration functions. In

the example, the failed disk was previously named *oracle10*, its current device address is *c3t5d2*, but in its normal address was *c3t3d1*.

- e. Note that some error conditions will not be noted as such in the *vxdisk list* command output. It is therefore recommended that the VM GUI be used to confirm the status of a disk drive.

11.3.2 Graphical User Interface Techniques. The VM GUI physical disk display provides a graphic depiction of the disk devices contained in an array that directly corresponds to the physical layout of disks within the array. In the VM physical disk display, failed devices in an array are indicated with a blue icon. In some configurations, the last disk in the first array is designated for swap use in an array-only configuration. This disk is not under VM control; therefore, it will appear as a failed device. This condition can be verified by examining the */etc/vfstab* file contents.

The layout of the disk icons in the view should match the layout of disks represented in the array front panel LCD display. The numbers specified on each physical disk (PD) icon provides the target (t#) and relative physical disk numbers (d#) in the following manner:

T0,D0	T2,D0	T4,D0
T0,D1	T2,D1	T4,D1
T0,D2	T2,D2	T4,D2
T0,D3	T2,D3	T4,D3
T0,D4	T2,D4	T4,D4
T1,D0	T3,D0	T5,D0
T1,D1	T3,D1	T5,D1
T1,D2	T3,D2	T5,D2
T1,D3	T3,D3	T5,D3
T1,D4	T3,D4	T5,D4

Front Side (Handle End)

For example, a device address containing *c#t3d1s#* for an array disk unit denotes a disk device located in the fourth slot from the front of the second tray.

Perform the following steps to view a display of physical disk devices for an array:

- a. Log in as **root**.
- b. Launch the VM root window:

/opt/vxva/bin/vxva&

- c. In the root window view, click the LEFT mouse button on the screen button corresponding to the four digit world number in the front panel LCD display on the array. This action produces a view of the disk devices contained in the referenced array.
- d. Note any disk icons displayed in blue.
- e. Close the window by clicking LEFT on the **File** option in the menu bar of the window, and selecting **Close**; Exit may be selected to end the VM GUI session.

(or)

- a. Log in as **root**.
- b. Launch the VM root window:

/opt/vxva/bin/vxva&

- c. In the root window view, click the LEFT mouse button on the screen button corresponding to the name of a disk group (e.g., *oracledg*).

The VM disk icons (denoted by "D") that are displayed appear in the order of their selection in the configuration building process: left to right, and top to bottom. The order of the device names (c#t#d#s#) under each icon should indicate how the first available disk was selected from the first target number, followed by the selection of the next available disk from the next target number, and so on, until all required disks were selected.

Considering this convention, a failed disk and an HS disk (if it has replaced a failed disk) can be identified by an illogical break in the order of the device names. When an HS replaces a failed disk, the HS disk icon is labeled with a "D" to indicate that it is no longer available as an HS disk.

A completely failed physical disk will not appear in this display. However, a configured volume may be displayed containing a plex with an error status (denoted by an abnormal coloration of the plex) to indicate a failed disk.

In the latter situation, the properties of the plex in question

must be examined to identify the failed disk. Display the properties for a plex by clicking LEFT on the plex name (e.g., vol02-01), then clicking the RIGHT mouse button.

In the Plex Properties window, the plex Kernel State indicates the availability of the plex; a disabled plex cannot be accessed. Volume properties may be examined in the same manner, but a disabled volume cannot be accessed. A value other than zero in the Number of IO Failures field is also indicative of a volume problem.

When error conditions are present in a plex or volume, the SA must identify the disk that is most likely the cause of the problem. This can be accomplished by displaying the properties of each subdisk within the plex. A value other than zero in the Number of IO Failures field in the properties view is indicative of a disk problem.

- d. The VM group window can be closed by clicking LEFT on the **File** option in the menu bar of the window, and selecting **Close**; Exit may be selected to end the VM GUI session.

11.4 Disk Replacement Scenarios

11.4.1 Overview of Procedures. Certain disk replacement procedures may be performed based on the configuration of the failed disk. After the failed disk has been identified, the SA must determine whether or not the failed disk belongs to a mirrored volume, and whether or not it has been replaced by an HS disk. The following general procedures should be performed when considering configuring a failed disk:

- a. If the disk is part of a mirrored volume, and the HS disk has kicked in or is not available:
 1. Remove or replace the failed disk. If an HS disk is not available, the volume can continue to operate on the mirrored complement of the failed disk.
 2. Restore the volume configuration to its normal state after installing a new disk.
- b. The disk is part of a mirrored volume; and the HS disk is available, but did not kick in:
 1. If a replacement disk is not readily available for installation, remove the failed disk to allow the HS disk to kick in.
 2. When the new disk becomes available, install it in the array at the location of the failed disk.

3. Restore the configuration to its normal state after installing the new disk.

(or)

1. If a replacement disk is available, take all HS disks offline (by changing their properties) to prevent them from kicking in.
 2. Replace the failed disk.
 3. Restore the configuration to its normal state.
 4. Place the HS disks back online.
- c. If the disk is part of a non-mirrored volume:
1. Remove the affected volume and its associated plexes and subdisks.
 2. Replace the failed disk.
 3. Rebuild the volume.
 4. Restore volume data using standard data restore functions, e.g., *ufsrestore*.

11.4.2 Hot Spare Disk Operations.

- a. In the root window view, click the LEFT mouse button on the screen button corresponding to the name of the desired disk group (e.g., *oracledg*) to produce a view of its VM volumes, plexes, and subdisks.
- b. Locate a disk icon labeled with 'PD' or 'HS' (physical disk or hot spare, respectively). Active HS disks in the group are labeled as 'HS'.
- c. Click LEFT on the disk icon to highlight it, then click the RIGHT mouse button to display its properties.
- d. At the 'Hot Spare' entry of the properties window: click LEFT on **Yes** to designate the disk as an HS disk. To deactivate it, click LEFT on **No**.
- e. To exit the window: click LEFT on Apply to effectuate changes or Cancel to discard the window without making any changes.

11.4.3 Volume Operations (Non-Mirrored Disk Configurations).

- a. In the group window view, select the volume containing the failed disk by clicking LEFT on its icon.
- b. Record the name of all disks that are a part of the volume in the order that they appear.
- c. Record the file system name assigned to the volume (displayed under the volume icon).
- d. From the Basic-Ops menu, select **Volume Operations**, then select **Remove Recursively**.
- e. Select **Okay** to proceed with the removal.
- f. The failed disk can now be physically replaced in the array.
- g. After a failed disk has been replaced in the configuration, the volume can be rebuilt. This is accomplished by performing the following steps:
 1. In the appropriate group window view, click RIGHT on the first required disk icon (as noted when removing the volume) to highlight its icon, then click MIDDLE on the remaining required disk icons.
 2. From the Basic-Ops menu, select **File System Operations**, then select **Create**, then select **Striped**.
 3. Complete and verify the contents of the Striped Volume Create window (with standard values for 1.05GB disk drives) as follows:

Volume name: xxx99 (e.g., vol03)
Volume size: 9999999s (number of disks times 2050272 followed by 's' for sectors)
Number of Columns: (Number of disks selected)
Stripe unit size: 72
Create file system: Yes
Mount file system: Yes
Mount point: /xxx/xxx (file system mount point)
Mount automatically: Yes (or No, as required)
 4. To exit the window: click LEFT on Apply to effectuate changes or Cancel to discard the window without making changes.

11.5 Disk Removal and Installation

11.5.1 Physical Disk Removal. Perform the following steps to remove a disk drive from a SPARCstorage array unit:

- a. Review all aspects of the configuration of the disk to be removed, including its location in the array.
- b. Advise users who are logged in of imminent system termination.
- c. Gracefully shut down the Oracle database, if applicable.
- d. As **root**, take the system down:

 # uadmin 2 0
- e. After system completes termination, power off the CPU.
- f. Power off the array unit and allow disk devices to spin down (approximately 1 minute).
- g. Remove the front panel of the array to gain access to the disk trays.
- h. Remove the tray containing the disk to be removed, by releasing the tray's handle. Pull the tray outward until it catches. Feel for the tray flapper located on the bottom, rear, center of the tray. Push the flapper upward while slightly pulling the tray to release it. Do not apply force to release the tray!
- i. After removing the tray, place it securely on a flat surface before attempting to remove a disk drive.
- j. Remove the desired disk using the handle located on the top of the disk. Use caution in handling the disk (in case it is not the correct disk to remove, and has to be reinstalled).
- k. If a replacement disk is available, it can be installed now in the location vacated by the failed disk. When installing a disk, seat it carefully by pressing on the SUN emblem and locking it using its handle.
- l. Replace the tray back into the array. Feel for the tray flapper, push the flapper upward while pushing the tray to insert the tray. Do not apply excessive force to insert the tray!
- m. Power on the array. The ready state of the array is indicated when the lines in the LCD display on the front

panel become visible for all installed disks. After achieving this ready state, wait at least two minutes before proceeding

- n. After waiting at least two minutes, power on the CPU.
- o. Restore the VM environment to its normal disk configuration.

11.5.2 Physical Disk Installation. Perform the following steps to install a disk device into a SPARCstorage Array unit:

- a. Review all aspects of the configuration of the disk to be installed, including its required location in the array.
- b. Advise users who are logged in of imminent system termination.
- c. Gracefully shut down the Oracle database, if applicable.
- d. As **root**, take the system down:

 # uadmin 2 0
- e. After system completes termination, power off the CPU.
- f. Power off the array unit and allow disk devices to spin down (approximately 1 minute).
- g. Remove the front panel of the array to gain access to the disk trays.
- h. Remove the tray containing the disk to be removed, by releasing the tray's handle. Pull the tray outward until it catches. Feel for the tray flapper located on the bottom, rear, center of the tray. Push the flapper upward while slightly pulling the tray to release it. Do not apply force to release the tray!
- i. After removing the tray, place it securely on a flat surface before attempting to install the disk drive.
- j. Install the disk in the desired location. Seat the disk carefully by pressing on the SUN emblem and locking it using its handle.
- k. Replace the tray back into the array. Feel for the tray flapper, push the flapper upward while pushing the tray to insert the tray. Do not apply excessive force to insert the tray!
- l. Power on the array. The ready state of the array is

indicated when the lines in the LCD display on the front panel become visible for all installed disks. After achieving this ready state, wait at least two minutes before proceeding.

- m. After waiting at least two minutes, power on the CPU.
- n. Modify the VM environment to include the new disk in its configuration.

11.6 Restoring VM Configurations

11.6.1 Restoring Hot Spare Configuration. The following steps are performed when a situation exists wherein a failed disk that was logically replaced in the configuration by an HS disk has been physically replaced with a new disk:

- a. Log in as **root**.
- b. Initiate the `vxdiskadm` menu process, enter the following command:

vxdiskadm

(At this point the `vxdiskadm` menu should appear)

- c. Enter **1** (add or initialize a disk) in response to "operation to perform".
- d. Enter **disk device** (c#t#d# of the new disk) in response to "disk device to add".
- e. Enter **n** in response to "wish to encapsulate".
- f. Enter **y** in response to "wish to initialize".
- g. Enter **none** in response to "which disk group".
- h. Enter **y** in response to "continue with operation".
- i. Enter **n** in response to "add or initialize another disk".

(At this point the `vxdiskadm` menu should appear)

- j. Enter **4** (remove a disk for replacement) in response to "operation to perform".
- k. Enter **disk name** (disk name, e.g., *oracle10*, assumed by HS disk; refer to previously recorded configuration information obtained in previous steps) in response to "disk name".

l. Enter **y** in response to "continue with operation".

m. Enter **n** in response to "remove another disk".

(At this point the *vxdiskadm* menu should appear)

n. Enter **5** (replace a failed or removed disk) in response to "operation to perform".

o. Enter **disk name** (same disk name specified in Step k) in response to "select a removed or failed disk".

p. Enter **device** (disk device specified in Step d, or press <ENTER> if specified default device is correct) in response to "choose a device".

q. Enter **y** (provided the specified operation scenario is correct) in response to "continue with operation".

r. Enter **n** in response to "replace another disk".

(At this point the *vxdiskadm* menu should appear)

s. Enter **1** (add or initialize a disk) in response to "operation to perform".

t. Enter **disk device** (c#t#d# of the HS disk) in response to "disk device to add".

u. Enter **y** in response to "wish to reinitialize c#t#d#".

v. Enter **group** (name of disk group for HS, e.g., *oracledg*) in response to "which disk group".

w. Enter **disk name** (name of designated HS disk, e.g., *spare01*) in response to "disk name".

x. Enter **n** in response to "add or initialize another disk".

y. Enter **y** in response to "preserve this disk as hot-spare".

z. Enter **y** (provided the specified operation scenario is correct) in response to "continue with operation".

aa. Enter **n** in response to "add or initialize another disk".

(At this point the *vxdiskadm* menu should appear)

bb. Enter **q** (exit from menus) in response to "operation to

perform".

11.6.2 Restoring Non-Hot Spare Configuration. The following steps are performed when a situation exists wherein a failed disk that was not logically replaced by an HS disk has been physically replaced with a new disk in the array:

- a. Log in as **root**.
- b. Initiate the `vxdiskadm` menu process:

 # vxdiskadm
- c. Enter **1** (add or initialize a disk) in response to "operation to perform".
- d. Enter **disk device** (c#t#d# of the new disk) in response to "disk device to add".
- e. Enter **n** in response to "wish to encapsulate".
- f. Enter **y** in response to "wish to initialize".
- g. Enter **group** (name of an associated disk group, e.g., *oracledg*) in response to "which disk group".
- h. Enter **disk name** (name of disk, e.g., *oracle10*) in response to "disk name".
- i. Enter **n** (or 'y', as required) in response to "preserve this disk as hot-spare".
- j. Enter **y** (provided the specified operation scenario is correct) in response to "continue with operation".
- k. Enter **n** in response to "add or initialize another disk".

 (At this point the `vxdiskadm` menu should appear)
- l. Enter **q** (exit from menus) in response to "operation to perform".
- m. Perform functions to rebuild the affected volume.

SECTION 12. GSORTS ADMINISTRATION

12.1 Downloading GSORTS Database

Unlike any other GCCS application, each site's GSORTS database is initialized and maintained remotely by the Pentagon's JEXACR GSORTS office. Each GCCS site need only request they do so.

The request is made to the GCCS Hotline for JEXACR to put a full, SECRET, GSORTS database at a site. From then on, the JEXACR office will handle all details and ongoing operational support of the GSORTS database, and the site will have the data available for retrieval.

Some services provided by JEXACR are:

- a. Initial download of a full GSORTS database to the site's database server.
- b. Execution of ORACLE scripts to load the GSORTS database into the GCCS Version 2.2 ORACLE structure, created when GSORTS' segments were installed on the site database server
- c. Twice-daily database update service.

To check on the GSORTS database status, a user can either use the GSORTS icon or go to an xterm and use *sqlplus*.

To use the GSORTS icon:

- a. Click on the **GSORTS** icon.
- b. Select **Options->Database Last Update**
- c. Look at the date. If not within the last day or two, then the database is not current. If the date is 19 January 1995 or earlier, it is likely that only the test database is loaded.

To use *sqlplus*:

- a. Start an xterm
- b. Input the following:

source /opt/bin/coraenv<return>
- c. Execute the following:

sqlplus /<return>

(assumes the user has the GSORTS role)

- d. Select **max(bupdate)** from *bide* table.
- e. Look at the date. If not within the last day or two, then the database is not current. If the date is 19 January 1995 or earlier, it is likely that only the test database is loaded.

12.2 Using CDROM Maps

GSORTS provides a mechanism to look at Defense Mapping Agency (DMA) Arc Digital Raster Graphic (ADRG) maps. Unlike other applications that require reading the ADRGs from CDROM and downloading to disk, GSORTS will immediately read and display the ADRG CDROM contents. In an operations center, the time (and disk) savings can be substantial.

Unfortunately, within the GCCS environment, and especially with Solaris Version 2.3, many problems at the operating system level conspire to make use of the CDROMs difficult. We do not yet have a formula that will ensure success in using CDROMs with GSORTS within GCCS.

There are several problems with CDROMs, GSORTS, and GCCS:

- a. The Solaris Version 2.3 Volume Manager (volmgr) takes over the control of mounting CDROMs.
- b. The nearest CDROM drive to a given user may require substantial UNIX-level work to be accessible by GSORTS.
- c. Old (pre-1989) ADRG CDROMs will not read correctly.

Addressing each problem in turn:

- a. The Solaris Version 2.3 volmgr usually will automount any CDROM put into the disk drive. This means that the user should not use the GSORTS **MapUtilities->AdrgMaps->New CDROM** menu item. Go directly to the **Open CDROM Map** selection. If there is a file name in the list box, then pick the name and everything will work normally. If not, then the troubleshooting process begins. Again, we do not have answers to all situations and cannot re-create all problems. The Solaris Version 2.3 volmgr is not completely characterized. Usually, the user has to do an "eject" command from an xterm.
- b. As a first attempt to use CDROM maps, be sure and try a CDROM drive connected physically as part of the SPARCstation 20 application server on which GSORTS is executing. Do not spend time trying to get an xterm SPARCstation 5's CDROM drive to be visible to GSORTS until a CDROM drive on the

machine on which the GSORTS software is executing works.

- c. If the ADRG CDROM is pre-1989, do not use it. Solaris Version 2.3 volmgr cannot read them.

A hint for troubleshooting:

Try doing operating system commands as **root**. For example, issue the command **eject** (to get the CDROM out). This will bypass permissions problems.

SECTION 13. **HARDWARE ADMINISTRATION**

13.1 **Fiber Distributed Data Interface**

Within GCCS, the Fiber Distributed Data Interface (FDDI) will be installed as a selected package (SUWnf) immediately after the core UNIX environment is installed. This package contains the drivers and system changes required to support FDDI. Every SUN SBUS card is currently shipped with a UTP interface installed. To prevent conflicts in the resolution of IP addresses and host names, each enabled network interface must be assigned a unique host name and IP address.

13.1.1 **Procedures for Installing FDDI Interface Software.**

- a. Preparation:
 1. Install core UNIX operating systems (recommended patches not as yet installed).
 2. Determine FDDI IP address (must be different from ethernet IP address if any).
 3. Determine FDDI host name (must be different from ethernet hostname if any).
 4. Connect MAC connector from SPARC to FDDI hub.
- b. Insert FDDI CDRom in drive.
- c. Log in as **root**.
- d. To install FDDI patch, execute the following:

```
# /usr/sbin/pkgadd -d /cdrom/fddi_3_0/Solaris_2.x
```

The following will appear on your screen:

The following packages are available:

```
1 SUWnf FDDI/S Driver/Utilities(sparc) 3.0
```

```
Select package(s) you wish to process (or "all" to process  
all packages). (default: all) [?,?,q]: 1 <Return>
```

- e. Specify the nf0 (FDDI) host name. This name must be different from the le0 (ethernet) host name:

```
What host name do you want to use for nf<inst>: <HOSTNAME>
```

- f. Specify the nf0 (FDDI) host name. This name must be different

from the le0 (ethernet) host name:

What ip address do you wish to use for <HOSTNAME>

- g. Do not specify the SunNet Manager daemons:

Do you want to start the SunNet Manager daemons for SunLink
FDDI/S at boot time? [n] [y,n,?,q] **n**

- h. Confirm the installation of files with *setuid/setgid* permission:

Do you want to install these setuid/setgid files [y,n,?,q] **y**

- i. Confirm the execution of the post-installation script with
superuser permission:

this package contains scripts which will be executed with
superuser permission during the process of installing the
package.

Do you want to continue with the installation [y,n,?] **y**

- j. Confirm that the installation was successful:

Installation of <SUNWnf> was successful.

- k. Terminate the *pkgadd* program:

The following packages are available:

1 SUNWnf FDDI/S Driver/Utilities
(sparc) 3.0

Select package(s) you wish to process (or "all" to process
all packages). (default: all) [?,??,q]: **q** <Return>

- l. Eject the CDROM:

eject cdrom

- m. Re-boot the system:

sync;sync;reboot

- n. Proceed with the installation of additional drivers, packages, or patches.

- o. Proceed with the installation of GCCS.

13.1.2 3800 Router Configuration (Example). The following text is provided to illustrate what should appear at the console as the user enters the commands to activate the FDDI interface of the router. This example was produced in the GCCS lab using the Synoptics 3000S Intelligent Hub, in which the router is named 'gccslab' and the configuration was already resident in the router. Text shown in **bold** is what is entered from the keyboard. Additional comments are shown in parentheses.

```
gccslab)en

Password:  (the password will not echo)
gccslab#sh flash
4096K bytes of Flash address space sized on CPU board.
Memory type is Flash.
File name/status
 0  xk09190z      (Currently utilized module)
 1  xk91450z      (FDDI module)
[1499584/4194304 bytes free/total]

gccslab#config t

Enter configuration commands, one per line.
Edit with DELETE, CTRL/W, and CTRL/U; end with CTRL/Z
no boot system flash xk09190z  (disable old flash module)
boot system flash xk91450z  (enable new module)
^Z  (exit configuration mode)

gccslab#
%SYS-5-CONFIG_I: Configured from console by console ()

gccslab#write mem
[OK]
gccslab#exit

gccslab con0 is now available

Press RETURN to get started.
```

13.2 Synoptics 300S Intelligent HUB Introduction

This subsection is provided to assist with the installation of the Synoptics 3000S Intelligent HUB. It provides several types of information:

- The purpose of the HUB - Notes relative to installation.
- Inventory - What and how many of each component to expect.
- Router Configuration - How to activate the FDDI router port.

- Network Management Module (NMM) Configuration - How to perform basic configuration.

In addition to the above information, there are also configuration examples for both the router and the NMM modules.

This subsection is intended as an aid to the installation teams in getting them online to a network that will facilitate server installation. It is not intended to be a complete manual for the Synoptics HUBs.

13.2.1 Purpose of the HUB. The FDDI components are intended solely for the connection of GCCS servers. Each server will be linked to the hub utilizing fiber connections in a single attached mode. It may be necessary to connect the SUN servers to one of the Ethernet boards until the FDDI connection cables are shipped to the site. If this is the case, there will be a 10baseT Ethernet host module provided for this purpose.

The FDDI connections cannot be accomplished at this time because the required cables are not yet available. Separate instructions for making these attachments will be provided when these cables are received.

The router is intended to be utilized to make the bridge between the token-passing protocol of the FDDI components and the CSMA/CD components of the Ethernet side. Although this is the primary purpose of the router, it can be utilized for additional functions if an additional interface is added.

The FDDI-to-router connections will be accomplished via the ports provided in the front of the hub. Patch cables will connect from the router port to one of the FDDI ports. These cables are not yet available but will be shipped with instructions when they are received.

The Ethernet Network Management modules only are provided for this installation. Although two are provided, only one is required and only one should be installed. A separate Ethernet segment may be set up at a later time, or the second module can be kept as a back-up.

The Ethernet components of the hub are intended for connection of either individual GCCS workstations, or LAN segments to which workstations are in turn attached. Ethernet connections can be made to individual workstations on an as-needed basis. The Ethernet host modules supplied should match the network infrastructure at the site.

13.2.2 Inventory. The Intelligent HUB inventory should include the items shown in Table 13-1.

Table 13-1. Synoptics 3000S Hub Components

Synoptics 3000S HUB Components		
Item	Quantity	Comments
3000S	1	Chassis only.
Power Supply	1	Install in right-most chassis slot.
3904	1 - 3	FDDI Host Module (Quantity varies by site)
3800	1	Router Card with 1 Ethernet Interface.
3809	1	FDDI Interface for 3800 Router (to be installed on the 3800 router card).
3313A	2	Ethernet Network Management Module. Only one of these cards should be installed with the initial installation.
3301	2	10baseT Ethernet Host Module. Included if site has existing 10baseT infrastructure or if it is required for interim server connections.
* 3304A	2	10baseFL Ethernet Host Module. Included only if site has existing infrastructure that is 10baseFL.
* This item is not included if there is no Ethernet fiber infrastructure at the site.		

A complete set of manuals for the hardware is included in the shipping containers, including a set of router manuals included with the Model 3800 router module. This router module is actually a CISCO Model 4000 router, and configuration is done accordingly.

Subassembly for boards to be inserted into the 3000S chassis is limited to the FDDI Personality module for the router. A complete set of detailed instructions is included with the module. Follow them carefully. If the installer is not comfortable with this type of work, and there is no member of the team who is comfortable doing this assembly, request assistance from the site POC for this equipment.

NOTE: The position of the boards in the chassis is unimportant, except for the power supply, which must be located in the far right position.

13.2.3 Configuration of 3800 Router Module. The router is present in this configuration to perform the translation between the FDDI and the Ethernet sides of the network. This document is not meant to detail how to configure CISCO routers, but is intended to augment a standard configuration that is assumed to be already in place.

In the hardware installation manual for the 3809 FDDI router Personality manual, there is reference to flash modules that must be loaded prior to being able to configure this interface. Specific steps for accomplishing this load are provided in Table 13-2.

Table 13-2. Configuration of 3800 Router

3800 Router Configuration		
#	Command	Description
1	en	Attach a terminal or a PC to the console port of the 3800 router module. Enter Enable mode. This requires a password.
2	sh flash	Display the file names currently stored in system flash memory. There should be two files shown; make note of both names. The first, (file 0) is the current image and the second, (file 1) is the one that must be used for FDDI.
3	config t	Enter configuration mode from the terminal.
4	no boot system flash xk09190z	Disable the old software module which does not include the FDDI driver. (file 0)
5	boot system flash xk91450z	Specify the proper file for enabling the FDDI interface. (file 1)
6	^z	Exit from configuration mode.
7	write mem	Write the new configuration to system memory.

Table 13-2. Configuration of 3800 Router (cont.)

8	exit	Exit from console. The FDDI interface can now be configured using standard configuration commands.
---	------	---

13.2.4 Configuration of 3313A Ethernet Network Management Module. The NMM for Ethernet can be configured with an IP address, and should be configured if network management is to be performed. The following sequence of steps in Table 13-3 details how to configure the NMM for Ethernet.

Table 13-3. Configuration of 3313A Ethernet NMM

3313A NMM Configuration		
#	Command	Description
1	^C	Connect cable to service port. Typing '^C' brings up the main menu (NOTE: the C is Capital.)
2	m	Toggle boot mode to EEPROM.
3	p	Toggle boot protocol to IP.
4	o	Toggle management protocol to IP.
5	i	Toggle image load mode to local.
6	j	Enter IP configuration menu.
7	a	Set IP address (obtained from site administrator).
8	a	Set default gateway (Same as defaultrouter in most cases).
9	<esc>	Exit back to boot mode menu.
10	w	Write boot config to EEPROM.
11	g	Execute power-up boot sequence; this will re-boot the module and display a banner requesting '^Y' for additional menu.
12	^Y	Enter load menu.
13	i	Enter the protocols parameter menu.
14	i	Enter IP parameters menu.
15	s	Set subnet mask (obtained from site administrator).
16	<look at screen>	Verify the correctness of IP information.

Table 13-3. Configuration of 3313A Ethernet NMM (cont.)

17	<esc><esc>	Return to main menu.
18	w	Write information to EEPROM.
19	z	Reset the 3313A.
20	<fini>	Remove the serial cable.

SECTION 14. CONFIGURING PCs TO DISPLAY DESKTOP

No single PC X-package or TCP has been selected for GCCS. Appendix B contains an evaluation of the leading X and TCP packages.

14.1 X-Package Installation

This section contains the screen captures of the options and selection for each of the X-packages evaluated. In all cases the installation selection should be "custom" or "selective" (as opposed to letting the package software automatically do the configuration). This non-automatic installation is required since all fonts must be installed.

14.1.1 Preparation for Installation. Prior to beginning installation, the following information should be gathered:

- Software Serial Number (if required by vendor)
- Authorization Code (if required by vendor)
- Network Software (TCP) Package Used
- Network Adapter
- Host Name
- Host IP Address
- Domain Name
- IP of Domain Name Server (DNS)
- Site Subnetwork

14.1.2 Screen Setups. The following pages show the screen setups for each of the X-packages evaluated.

14.1.3 XoftWare/32 . XoftWare/32 has a single menu that appears when its desktop icon is clicked on. The customization of the appearance and operation of XoftWare/32 is via the Options menu. Select **Options** from the main menu to access these features. Figure 14-1 provides screen captures of the options and selections.

Display

Window Mode

☐ Single-Window

☐ Enable Panning ☐ Display Scroll Bar

Virtual Screen: x

☒ Multiple-Window

☒ Enable Panning ☒ Motif Properties

☒ X Root Background ☒ Cascade Windows

☒ Prompt for Closing a Client

☒ Windows Keyboard Focus Policy

☒ Allow Concurrent Window Manager

☒ Fit Window to Display

Screen Visual:

☐ Reserve Windows System Colors

☐ Make Cursor Visible

Display Number:

Screen Dimensions in Millimeters

Width: Height:

OK Cancel Help

Server Features

Screen Saving

Backing Store:

☒ Save Unders

☒ X11R3 Bug Compatibility

☐ Exit Server with Closing of Last Client

☐ Disable Server Reset

☒ Prompt Before Closing Server

☒ Server Input Control Over Windows

☒ Enable Plane Mask

☒ Fast Line Drawing

☐ Preserve Restricted Colors

Data Files

RGB Colors File:

Log File:

Language:

OK Cancel Help

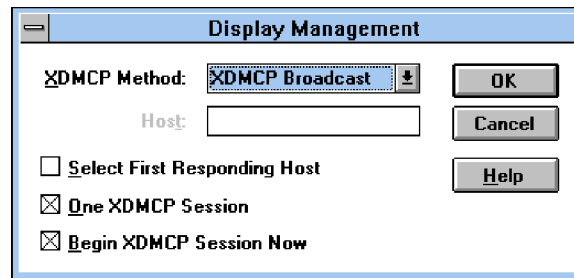


Figure 14-1. XoftWare/32 Screen Captures

14.1.4 PC-Xware. PC-Xware allows customization of features governing the way the X server operates. To configure the PC-Xware configuration options, select the **Configure - Xserver** tab. Figure 14-2 provides screen captures of the options and selections.

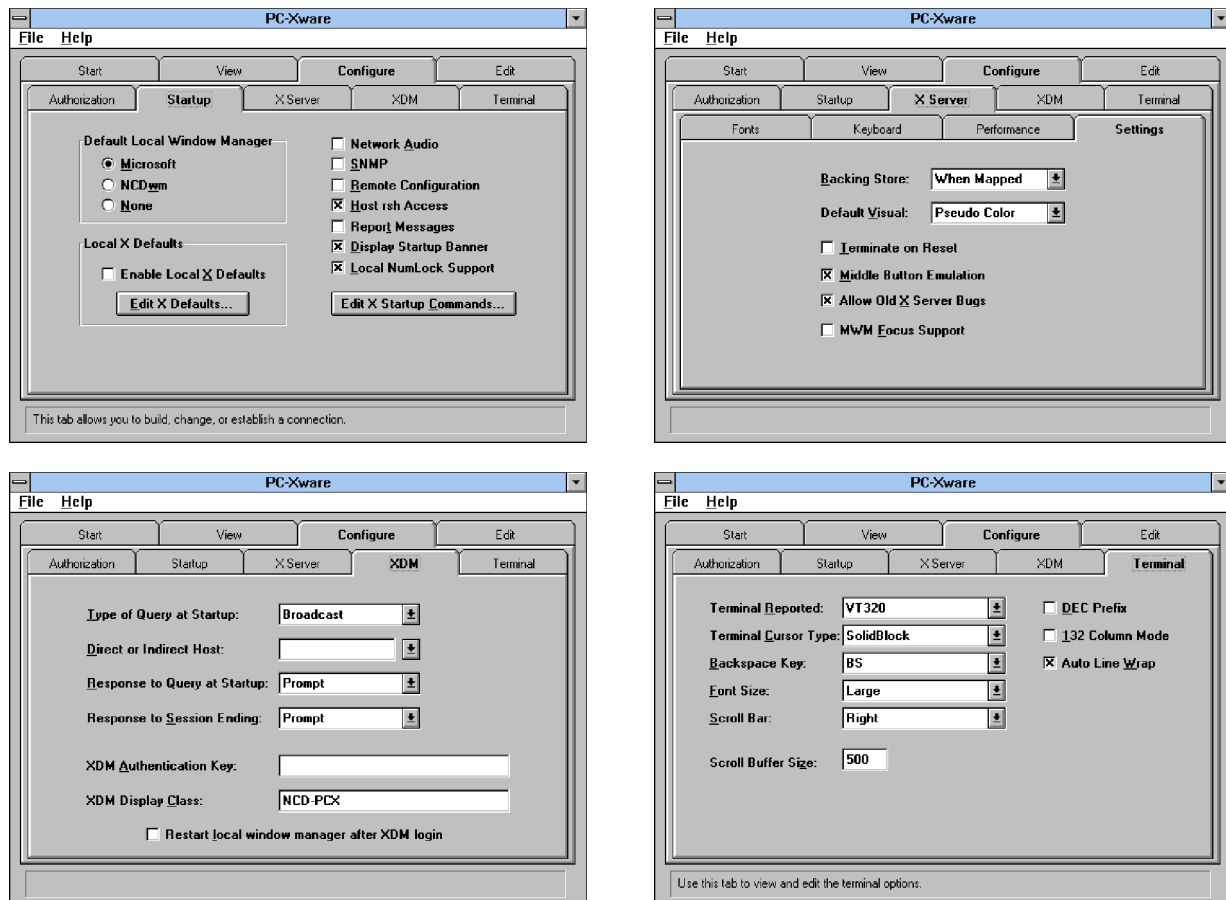


Figure 14-2. PC-Xware Screen Captures (1 of 2)

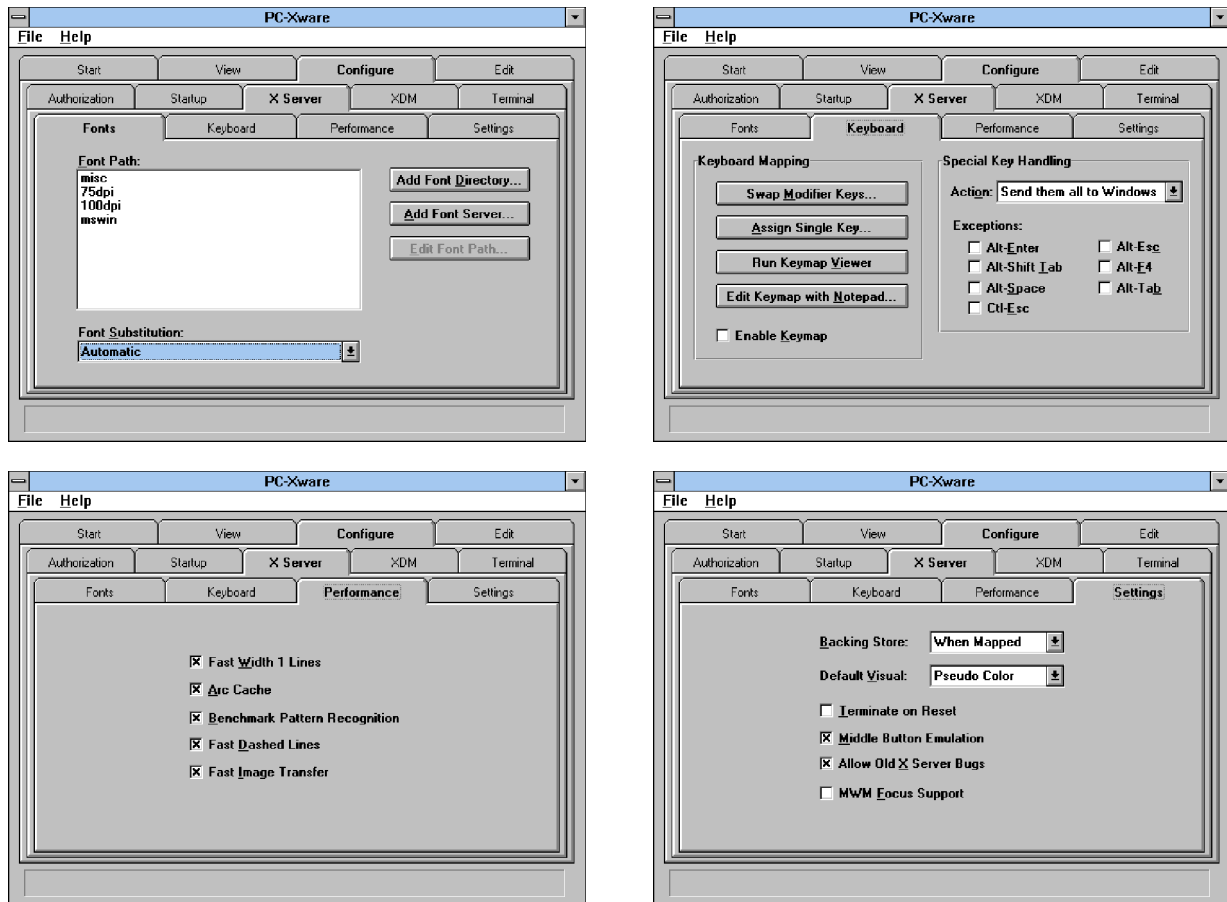


Figure 14-2. (2 of 2)

14.1.5 eXceed 4 for Windows. To configure eXceed 4 Windows features, start the "Xconfig" program. A dialog box is displayed, displaying icons for each type of setting or function available. Figure 14-3 provides screen captures of the options and selections.

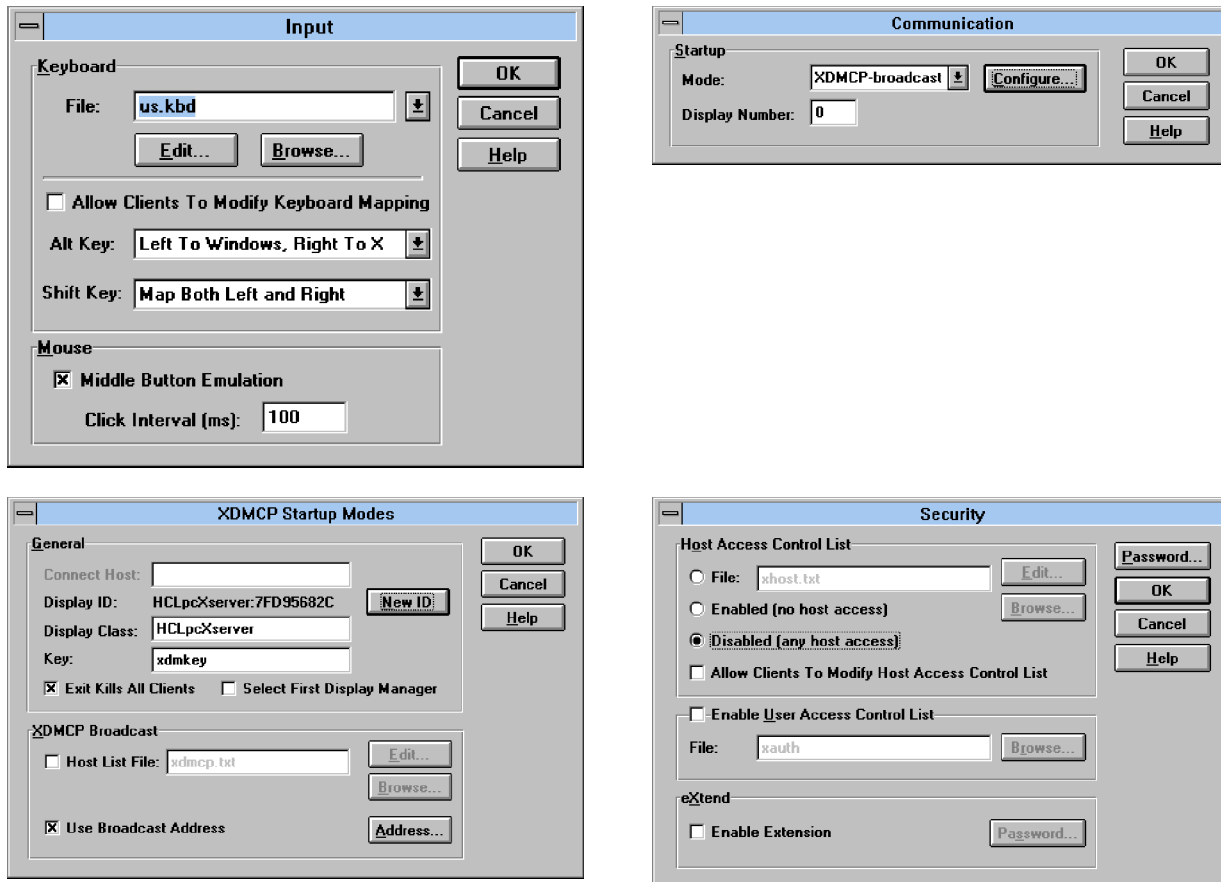


Figure 14-3. eXceed 4 Windows Screen Captures (1 of 2)

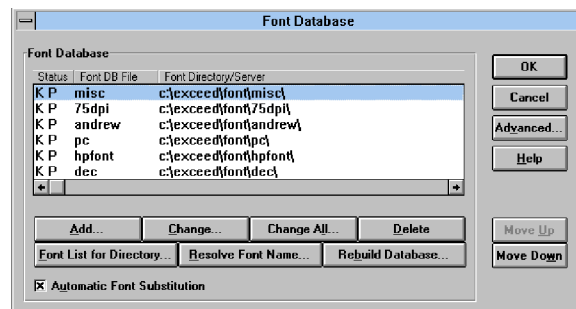
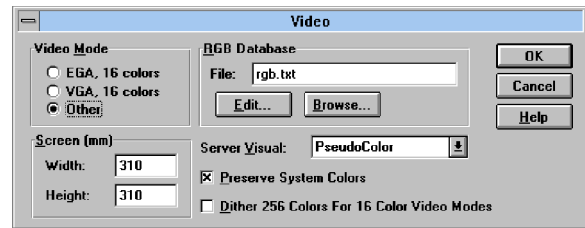
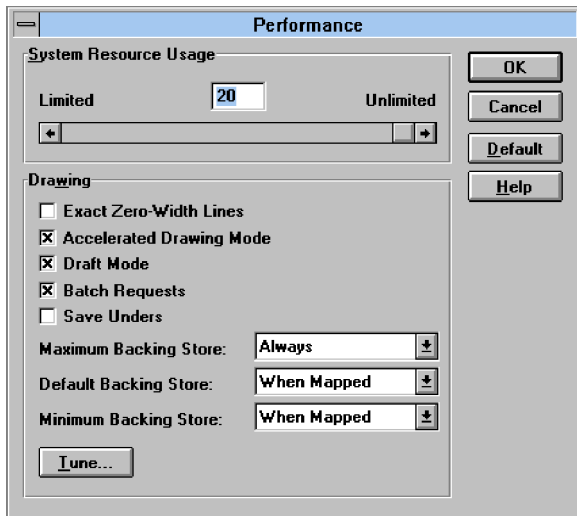
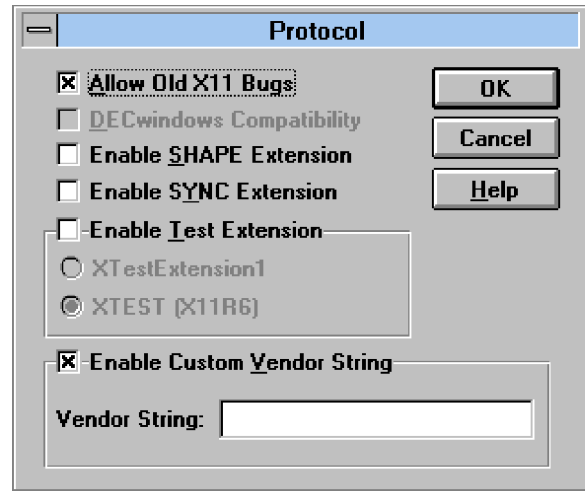
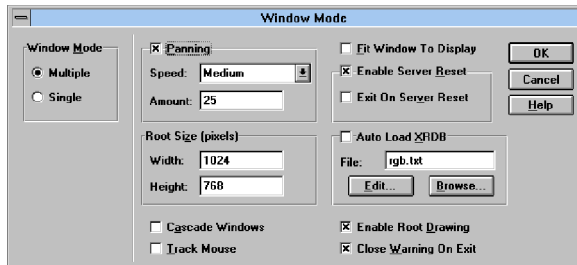


Figure 14-3. (2 of 2)

14.1.6 Reflection-X. Reflection-X allows customization of features governing the way the X server operates by selecting the tools option from the desktop icon. Then select the icon of the feature to configure. Figure 14-4 provides screen captures of the options and selections.

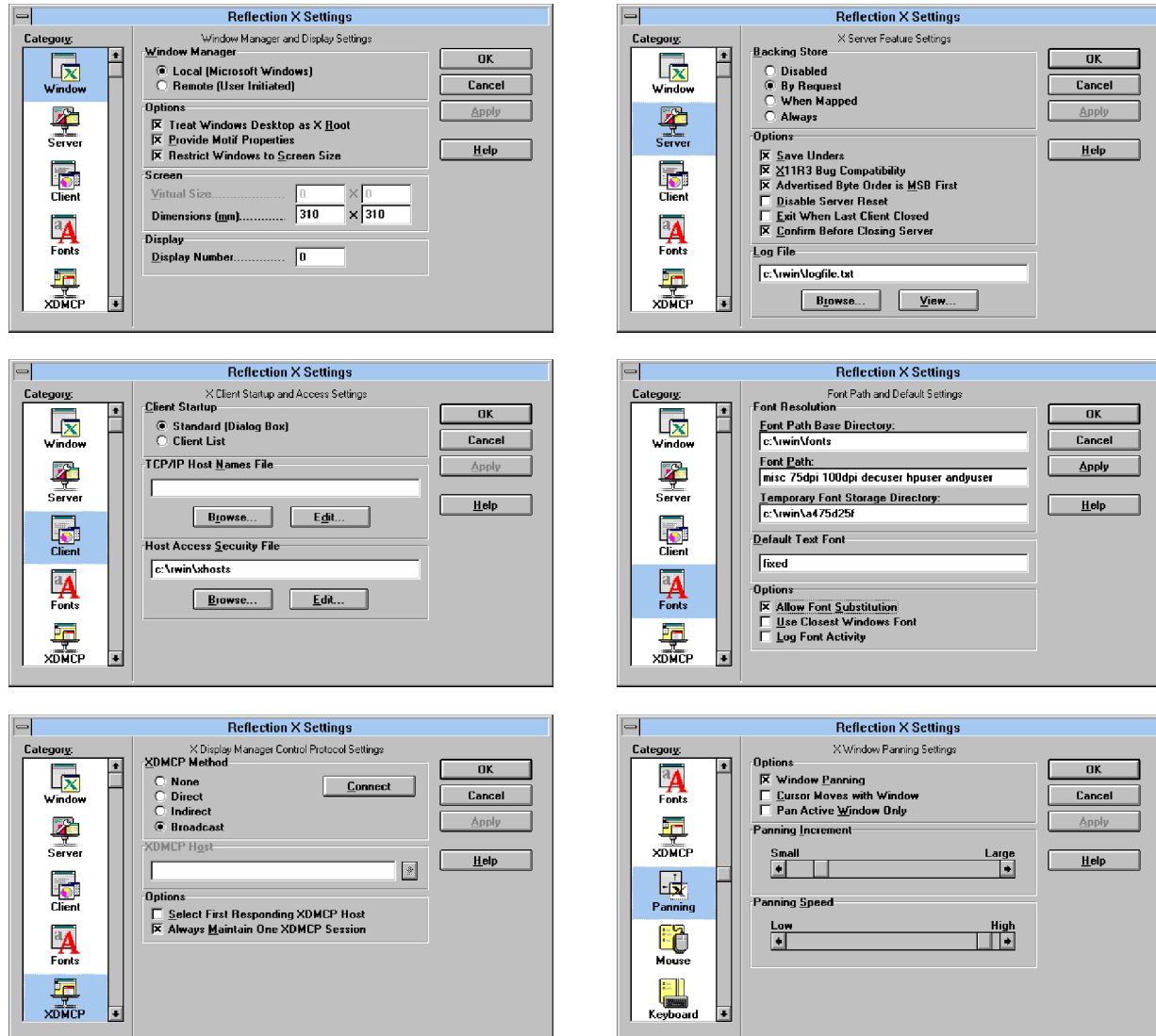


Figure 14-4. Reflection X Screen Captures (1 of 2)

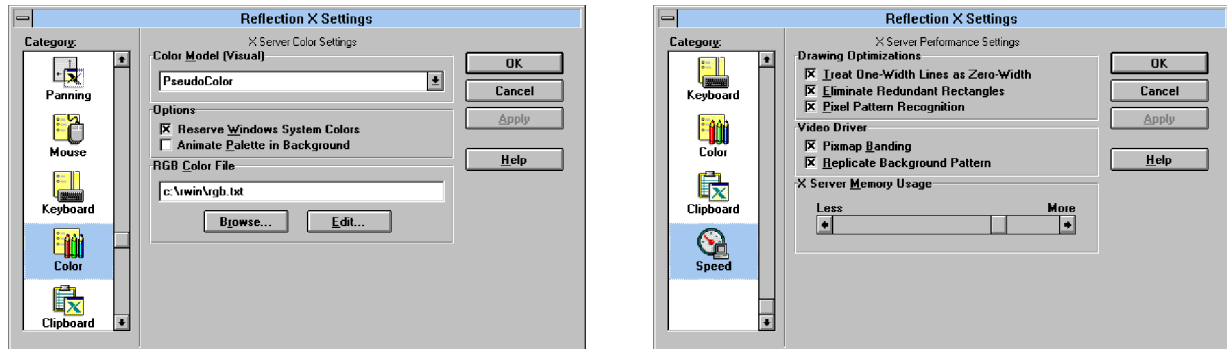


Figure 14-4. (2 of 2)

14.1.7 Xvision. The Xvision Control Panel allows configuring of the server without starting an X session. Click the right mouse button over the **Xvision Control Panel**. Choose the menu command that contains the option to be changed. Figure 14-5 provides screen captures of the options and selections.

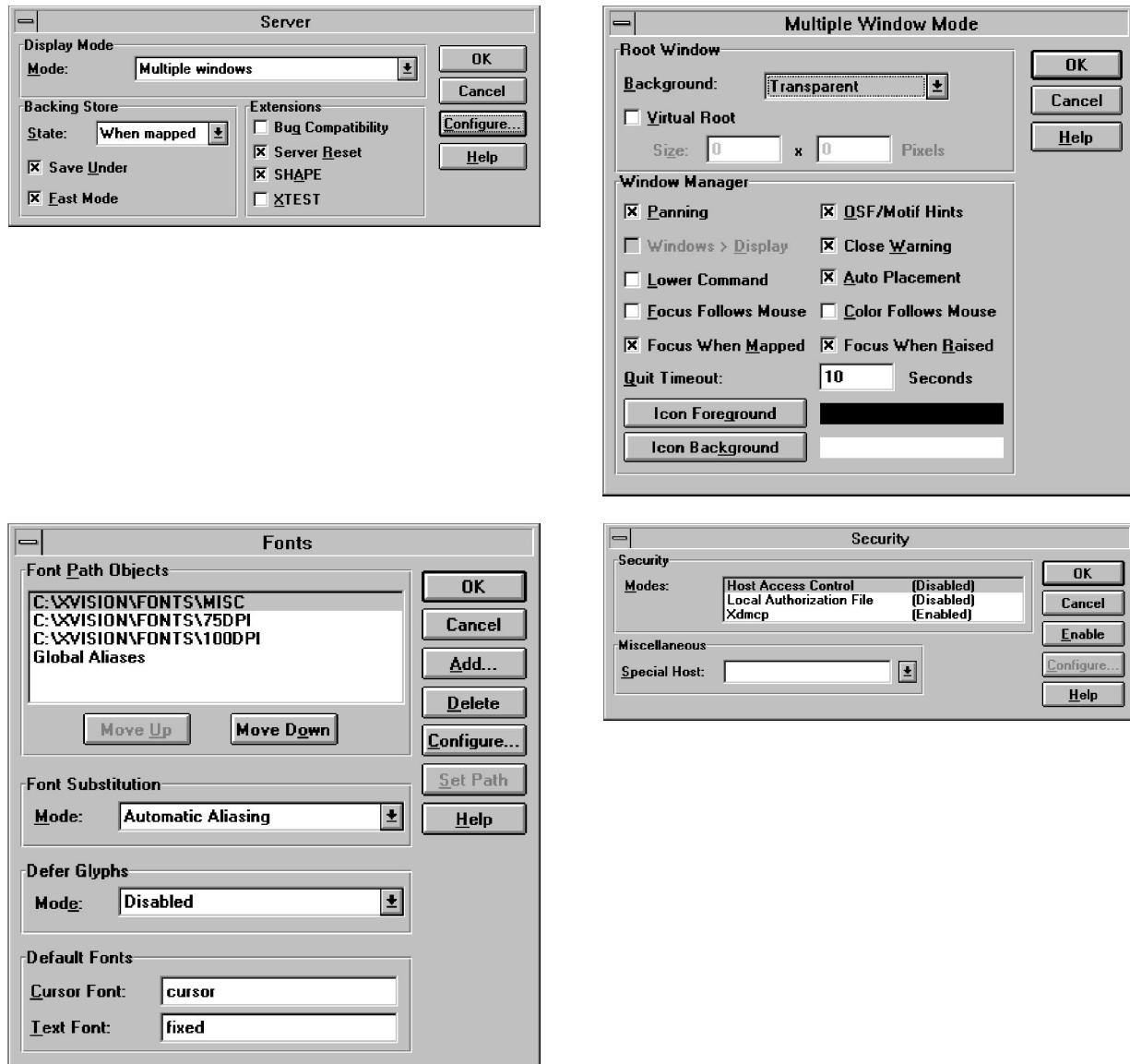


Figure 14-5. Xvision Screen Captures (1 of 2)

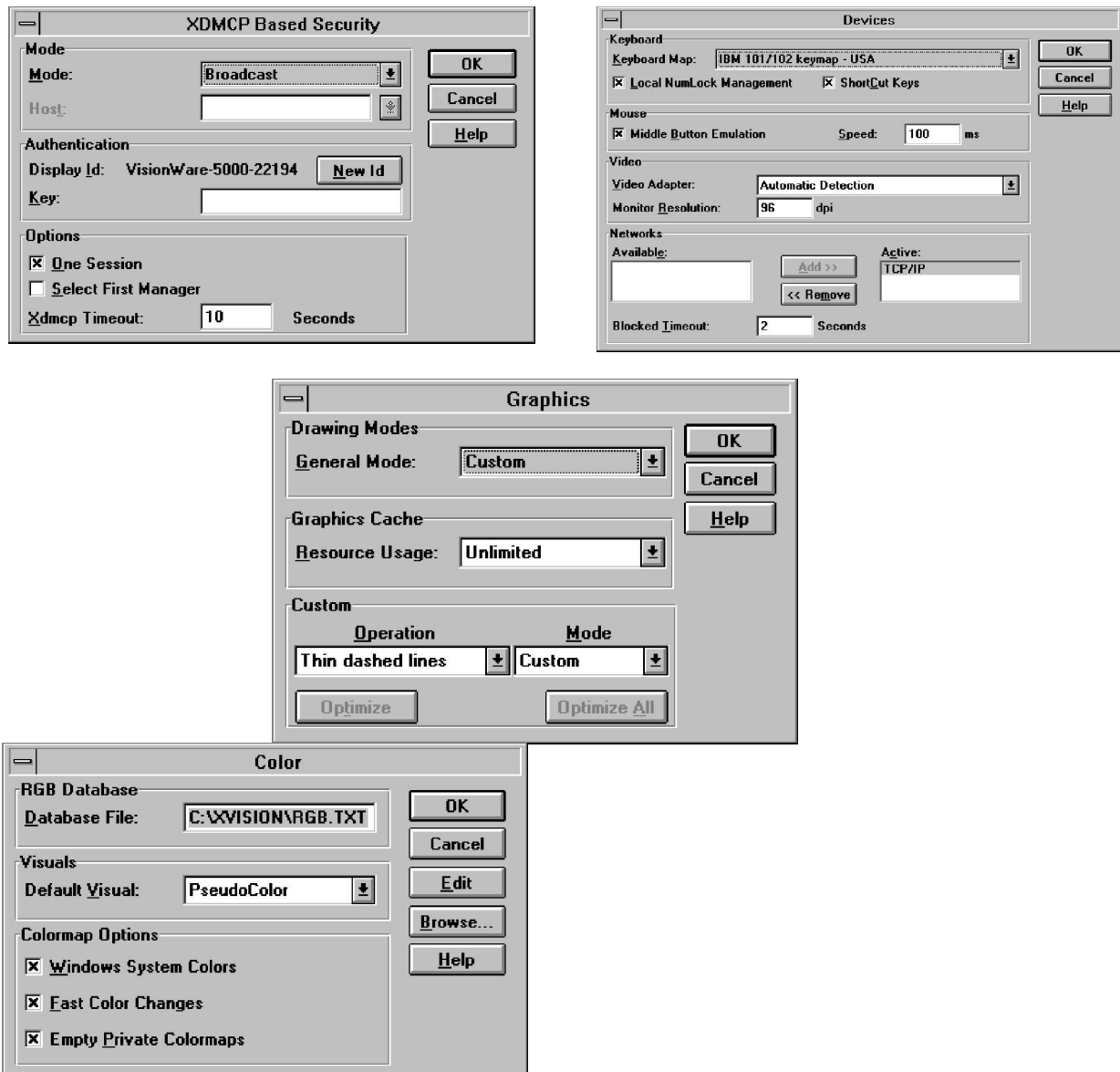


Figure 14-5. (2 of 2)

SECTION 15. INFORMATION MANAGEMENT SUBSYSTEM/REFERENCE FILE MANAGER (IMS/RFM) ADMINISTRATION

IMS/RFM administration consists of entering the appropriate script names and file paths into config files—one for IMS and one for RFM. The scripts are executed when the IMS and RFM tools are used.

15.1 IMS Admin Tool

The IMS Admin Tool icon launches the IMS configuration function. This function should be used only by designated personnel in accordance with site procedures. IMS controls the Time-Phased Force and Deployment Data (TPFDD) data transfer facility, and is the centralized TPFDD data management interface among DART, JFAST, and the JOPES Core Database.

15.1.1 Who Can Run the IMS Admin Tool. As currently configured, only the user ID who is the owner of the `/h/IMS_RFM/bin/ims_apps` file can start the IMS Admin Tool. By default, the user ID is IMSRM. This means that to use the IMS Admin Tool, a user must log onto it as **IMSRM**.

15.1.2 How to Recover the Original IMS Configuration. If changes need to be made to the IMS operational configuration (the scripts and path names stored in `/h/IMS_RFM/bin/ims_apps` file using the IMS Admin tool), then the user needs to copy the backup file called `ims_apps.real` to the file name `/h/IMS_RFM/bin/ims_apps`.

15.2 RFM

The Reference Manager Administration Tool icon launches the RFM configuration function. To ensure proper management of standard reference files, this function should be used only by designated personnel in accordance with site procedures. RFM is the reference file transfer manager. The Reference Manager icon launches the RFM process, and causes the RFM Command screen to be displayed, for standard reference file transfers. This function should be used only by designated personnel in accordance with site procedures.

RFM allows the user to acquire and transfer JOPES standard reference files (such as ASSETS, CHSTR, GEOFILE, TUCHA) required for operation planning. RFM gets the reference files from the JOPES Core Database when the RFM Update button is used for a given reference file.

15.2.1 Who Can Run the RFM Admin Tool. As currently configured, only the user ID who is the owner of the `/h/IMS_RFM/files/refapp_info` file can start the Refman Admin Tool. By default, the user ID is IMSRM. This means that to use the RFM Admin Tool, a user must log onto it as **IMSRM**.

15.2.2 How to Recover the Original RFM Configuration. If changes need to be made to the RFM operational configuration (the scripts and path

names stored in */h/IMS_RFM/files/refapp_info* file using the RFM Admin tool), then the backup file called *refapp_info.real* must be copied to the file name *refapp_info*.

SECTION 16. CHANGING IP ADDRESSES AND HOST NAMES

16.1 Changing IP Addresses on SPARCstations

When a site finds it necessary to change the IP address of a SPARCstation(s), there are several files both on the affected SPARCstation and on other platforms that may require modification. Perform the following steps using the editor of your choice on the SPARCstation for which the IP address is being changed:

- a. Deactivate NIS+ on the SPARCstation by executing the following (see also Section 6 of this Manual):

```
# cd /var/nis<return>
# rm -rf * <return>
# rm /etc/defaultdomain <return>
# rm /etc/.rootkey <return>
# ps -ef | grep nis <return>
```

Note the process ID (PID) for:

```
/usr/sbin/rpc.nisd -r
/usr/sbin/nis_cachemgr
```

```
# kill -9 {PID} {PID}<return>
```

- b. If changing the IP address of the ORACLE database server, de-install the DART application.
- c. In the `/etc/inet/hosts` file change the IP address for the SPARCstation being modified.

Example: 164.117.210.166 brady

- d. In the `/etc/inet/netmasks` file, change the network number and the netmask if necessary. Both numbers are written in "decimal dot" notation and should be obtained from your network administrator.

Example: 164.117.0.0 255.255.255.0

- e. In the `/etc/inet/networks` file, change the broadcast address to that of the Executive Manager.

Example: subnet1.gccs 164.117.210.255

This address can be determined by running the following command on the EM server:

ifconfig ??? where ??? is the ethernet port number of SPARCStation, e.g., le0, ie0

- f. If the IP address of the default router has changed, modify the following file accordingly:

`/etc/defaultrouter`

- g. If the IP address and/or the DNS domain name have changed, modify the `/etc/resolv.conf` to reflect this.

Example: domain ims.disa.mil
 namserv 164.117.210.64

- h. Re-boot the system.
- i. If this is the ORACLE database server, install the DART application.
- j. Refer to Section 16.3 for changes required to NIS+ and DNS.

16.2 Changing the Host Name of a SPARCstation

When it is necessary to change the host name of a SPARCstation(s) there are several files both on the affected SPARCstation and on other platforms that may require modification. Perform the following steps using the editor of your choice on the SPARCstation whose host name is being changed:

- a. Deactivate NIS+ on the SPARCstation by executing the following (see also Section 6 of this Manual):

```
# cd /var/nis <return>
# rm -rf * <return>
# rm /etc/defaultdomain <return>
# rm /etc/.rootkey <return>
# ps -ef | grep nis <return>
```

Note: the process ID (PID) for:

```
/usr/sbin/rpc.nisd -r
/usr/sbin/nis_cachmgr
```

```
kill -9 {PID} {PID}<return>
```

- b. If changing the host name of the ORACLE database server, de-install the DART segment.

- c. In the */etc/inet/hosts*, file change the host name for the SPARCstation being modified.

Example: 164.117.210.166 brady

- d. In the */etc/nodename* file, change the host name entry to the new host name.
- e. In the */etc/hostname.???* (where ??? is the ethernet port of the SPARCstation, e.g., */etc/hostname.le0*) change the host name entry to the new host name.
- f. In the */etc/net/ticlts/hosts* change all occurrences of the old host name to the new host name.
- g. In the */etc/net/ticots/hosts* change all occurrences of the old host name to the new host name.
- h. In the */etc/auto_home* file change all occurrences of the old host name to the new host name.
- i. Execute the following:

```
# mv  /.xsun.{old hostname}:0  /.xsun.{new hostname}:0
```

- j. All occurrences of the old host name in the users *.rhosts* file will have to be changed to the new host name. The *.rhosts* are located in the following directories:

```
/h/USERS/{user id}/Scripts
```

- k. If changing the host name of the Executive Manager server changes any occurrence of the old host name to the new host name in the following files:

```
/h/EM/admin/security-scripts/security-servers  
/h/data/global/EMDATA/config/active_spt  
/h/data/global/EMDATA/config/processor_table
```

- l. Re-boot the system.
- m. Refer to Section 16.3 for changes required to NIS+ and DNS.
- n. If this is the ORACLE database server, install the DART segment at this point.

16.3 Changes Required to NIS+ and DNS when Changing Host Names and IP Addresses

After all the system files have been modified on the SPARCstation whose

IP address and/or host name is being changed the NIS+ database will have to be update to reflect the change. To do this, execute the procedures in Section 6.3.3 of this Manual.

If the IP address of the NIS+ server has been changed the NIS+ server will have to be reconfigured (see Section 6.3.1 of this Manual), as will all the clients.

Any change of a host name and/or IP address requires a change to the DNS nameserver database. Consult Section 5 of this Manual "DNS Administration" for the procedures on modifying the nameserver tables.

16.4 Changing IP Address and/or Host Name on Sybase Server

If the host name and/or IP address of the Sybase server is changed, the "interfaces" file located in `/h/COTS/SYBASE` must be updated, since it contains both the host name an IP address (in hexadecimal). To do this, execute the following on the Sybase server:

- a. Log in as **root** and change the host name of the Sybase server found in the `/etc/inet/hosts` to a dummy name.
- b. Add the new IP address of the Sybase server followed by the host name to the `/etc/inet/hosts` file.
- c. Execute the following:

```
# su - sybase <return>
# cd /h/COTS/SYBASE/install <return>
```
- d. Modify the IP address by executing the following:

```
# sybinit <return>
```

The following output will appear:

```
The log file for this session is
'/home1/COTS/SYBASE/init/logs/log0801.001'.
```

```
SYBINIT
```

1. Release directory: `/h/COTS/SYBASE`
2. Edit / View Interfaces File
3. Configure a Server product
4. Configure an Open Client/Server product

```
Ctrl-a Accept and Continue, Ctrl-x Exit Screen, ? Help.
```

Enter the number of your choice and press return:

e. Enter the following:

2 (Edit / View Interfaces File)

followed by a <return>.

The following output will appear:

INTERFACES FILE TOP SCREEN

Interfaces File:

1. Add a new entry
2. Modify an existing entry
3. View an existing entry
4. Delete an existing entry

Ctrl-a Accept and Continue, Ctrl-x Exit Screen, ? Help.

Enter the number of your choice and press return:

f. Enter the following:

2 (Modify an existing entry) followed by a <return>.

The following output will appear:

CHOOSE INTERFACES FILE ENTRY

Select one of the following interfaces entries:

1. SYB_BACKUP
2. GCCS

Ctrl-a Accept and Continue, Ctrl-x Exit Screen, ? Help.

Enter the number of your choice and press return:

g. Enter the following:

1 (SYB_BACKUP) followed by a <return>.

The following output will appear:

SERVER INTERFACES FILE ENTRY SCREEN

Server name: SYB_BACKUP

1. Retry Count: 0
2. Retry Delay: 0
3. Add a new listener service

Modify or delete a service

Listener services available:

	Protocol	Address	Port	Name Alias
4.	tcp	brady	6500	

Ctrl-a Accept and Continue, Ctrl-x Exit Screen, ? Help.

Enter the number of your choice and press return:

- h. Enter the following:

4 (Protocol Address Port Name Alias)followed by
<return>.

The following output will appear:

EDIT TCP SERVICE

1. Hostname/Address: brady
2. Port: 6501
3. Name Alias:

4. Delete this service from the interfaces entry

Ctrl-a Accept and Continue, Ctrl-x Exit Screen, ? Help.

Enter the number of your choice and press return:

- i. Enter the following:

1 (Hostname/Address)followed by <return>.

The following output will appear:

Enter the hostname or Internet address to use for this entry
(default is 'brady'):

- j. Enter the following:

{IP address}

or

{hostname} followed by a <return>.

The following output will appear:

```
1.  Hostname/Address:  hostname
2.  Port:  6501
3.  Name Alias:

4.  Delete this service from the interfaces entry

Ctrl-a Accept and Continue, Ctrl-x Exit Screen,  ?  Help.

Enter the number of your choice and press return:
```

k. Enter:

Ctrl-a (Accept).

l. Enter:

Ctrl-x

m. Enter the following:

Ctrl-x

The following output will appear:

```
CHOOSE INTERFACES FILE ENTRY

Select one of the following interfaces entries:

1.  SYB_BACKUP
2.  GCCS

Ctrl-a  Accept and Continue,  Ctrl-x Exit Screen,  ?  Help.

Enter the number of your choice and press return:
```

n. Enter the following:

2 (GCCS) followed by a <return>.

The following output will appear:

```
SERVER INTERFACES FILE ENTRY SCREEN

Server name:  SYB_BACKUP

1.  Retry Count:      0
```

2. Retry Delay: 0

3. Add a new listener service

Modify or delete a service

Listener services available:

	Protocol	Address	Port	Name Alias
4.	tcp	brady	6500	

Ctrl-a Accept and Continue, Ctrl-x Exit Screen, ? Help.

Enter the number of your choice and press return:

o. Enter the following:

4 (Protocol Address Port Name Alias) followed by
<return>.

The following output will appear:

EDIT TCP SERVICE

1. Hostname/Address: brady
2. Port: 6501
3. Name Alias:

4. Delete this service from the interfaces entry

Ctrl-a Accept and Continue, Ctrl-x Exit Screen, ? Help.

Enter the number of your choice and press return:

p. Enter the following:

1 (Hostname/Address)

followed by <return>.

The following output will appear:

Enter the hostname or Internet address to use for this entry
(default is 'brady'):

q. Enter:

the new **IP address** or **hostname**

followed by a <return>.

The following output will appear:

1. Hostname/Address: hostname
 2. Port: 6501
 3. Name Alias:
 4. Delete this service from the interfaces entry
- Ctrl-a Accept and Continue, Ctrl-x Exit Screen, ? Help.
- Enter the number of your choice and press return:
- r. Enter the following:
- Ctrl-a** (Accept).
- s. Enter the following:
- Ctrl-x** until the command line prompt is displayed.
- t. Type:
- exit** to return to root.
- u. Execute the following on the new *interfaces* file to make it available to all GCCS platforms:
- ```
cp /h/COTS/SYBASE/interfaces /h/data/global/EMDATA/sybase
```
- v. In the */h/COTS/SYBASE/install/gccs.rs* file change the host name entry at the end of the following line:
- ```
sqlsrv.network_hostname_list: {hostname}
```
- w. In the */h/COTS/SYBASE/install/gccs_Backup.rs* file change the host name entry at the end of the following line:
- ```
bsrv.network_hostname_llist: {hostname}
```
- x. Change any occurrence of the old host name to the new host name in the following files:
- ```
/h/data/global/EMDATA/config/active_spt  
/h/data/global/EMDATA/config/processor_table
```

SECTION 17. UPS ADMINISTRATION

Uninterruptible Power Supply (UPS) systems are designed to provide AC input power protection to attached equipment, against a variety of irregular power conditions. These power conditions can range from power spikes to a total power outage, causing hardware damage or loss/corruption of data. To mitigate administration down-time in the event of a unwanted power condition as described above, UPSs have been provided.

Effectively providing reliable power conditioning for a system requires that the total system load requirements must first be determined. Once system load and power consumption has been determined, the correct UPS model can be selected to provide regulated and filtered incoming AC power to the attached system. This is accomplished by identifying all equipment that must have power protection, and the peak power consumption for each device as specified by the equipment manufacturer. For the known various GCCS configurations, the recommended configuration is that the UPS connected to the CPU should also have connected to it the monitor and as many primary external support drives as possible. After determining the best possible configuration for the system connections, proceed to Section 17.2, "Hardware Installation."

17.1 Related Documents

- UPSI Operations Manual
- OnliSafe Power Manual

17.2 Hardware Installation

This section will guide the installer through unpacking and operational configuration of the UPSI UPS 800ext-1500ext models.

1. ***** IMPORTANT ***** Read the safety instructions contained on pages 7-9 in the *UPSI Operations Manual*.
2. Unpack and inspect the UPS as described on page 41 of the *UPSI Operations Manual*.
3. Connect the power cord to the UPS input power connector located on the rear panel of the UPS. Do not connect the power cord(s) of the protected equipment into the power output receptacles at this time. Plug the UPS power cord into a grounded house power receptacle and watch the UPS control panel indicators. After the UPS cycles through internal power up diagnostics, indicators I1 (green) and I7 (amber) will remain illuminated (see Figure 17.1). This condition indication is normal UPS operational condition exists. If the UPS does not switch to the normal operational mode immediately remove AC input power from the UPS and refer to the Error Conditions section on page 53 in

the *UPSI Operations Manual*.

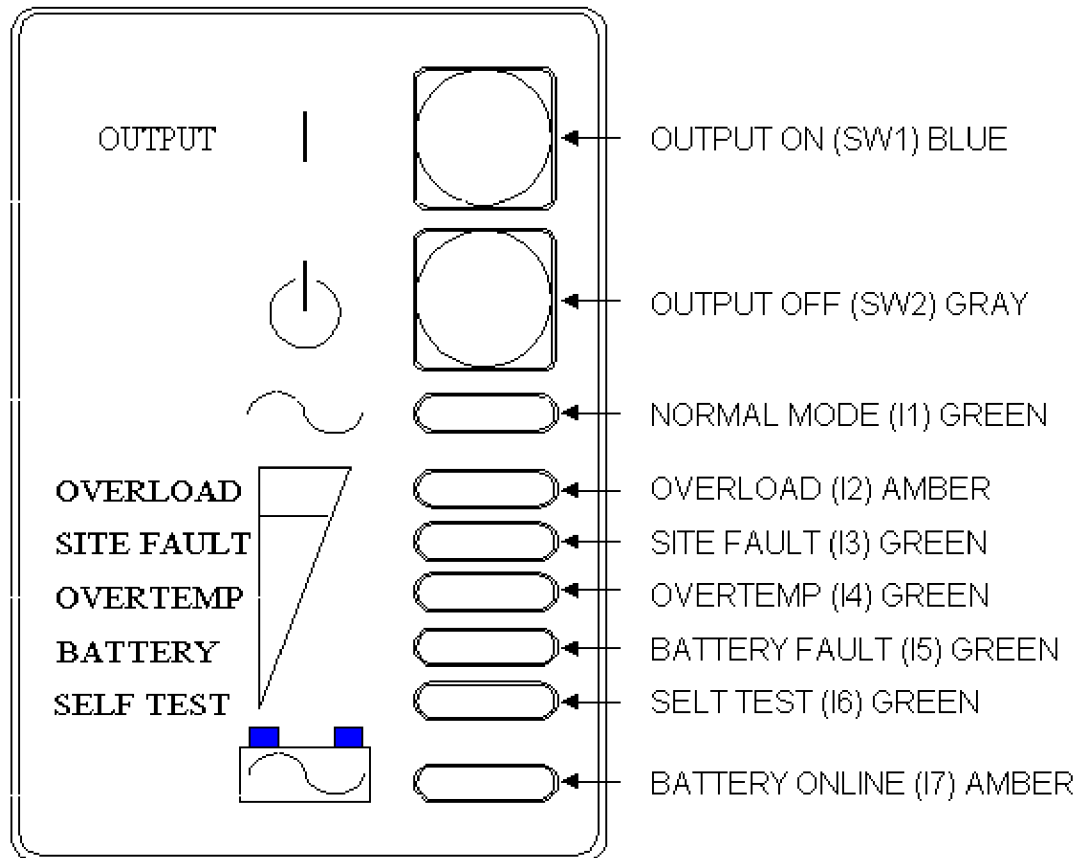


Figure 17-1. UPS Front Panel Controls and Indicators

4. The UPS is equipped with an external communications port used to communicate with the SPARC computer running OnliSafe power management software. To allow computer to UPS communications will require reconfiguration of the UPS communications port from the factor default configuration. The steps provided below will reconfigure the UPS port to the AS/400 configuration. It is recommended that the installer reviews the steps below before proceeding with the installation. The UPS has a configuration time limit, which, if exceeded, will require the steps to be performed repeatedly until performed correctly in a timely manner.
 - a. Unplug the UPS AC input power from house power.
 - b. Plug the UPS AC input power into house power while pressing the UPS Output OFF (SW2) on the UPS front panel until the alarm beeps (see Figure 17.1). All indicators

will begin to flash on and off.

- c. Immediately press the Output OFF (SW2) on the UPS front panel until the alarm beeps again. The I3 factor default configuration indicator will begin to flash on and off.
- d. Immediately press the Output OFF (SW2) on the UPS front panel one time or repeatedly until the I4 indicator begins to flash on and off.
- e. Immediately press the Output ON (SW1) on the UPS front panel until the alarm beeps, and then press the Output ON (SW1) a second time. The UPS will switch to the normal operational mode.
- f. The configuration can be verified by performing Steps a through c again.
- g. After successful completion of the hardware installation, the protected equipment can be plugged into the power output receptacles located on the rear of the UPS.
- h. Proceed to Section 17.3, OnliSafe Powerware Software Installation.

NOTE: If the site needs further assistance, contact:

Universal Power Systems, Inc.
11200 Waples Mill Road, Suite 350
Fairfax, Virginia 22030
(800) 438-8774
(703) 352-8644

17.3 OnliSafe Powerware Software Installation

The UPS is equipped with a communications port used to communicate with computers running OnliSafe power management software. The power management software has been preconfigured and segmented for installation onto a GCCS SPARC system running Solaris 2.3/SunOS 5.3. Prior to installing the UPSI Segment Version 1.3, "Powerware OnliSafe Solaris (SPARC) V 3.1.2 software," the installation instructions in Section 17.2, "Hardware Installation," should be performed. If the hardware installation has not been implemented, the system should be shut down and disconnected from the UPS, and the installation instructions in Section 17.2 "Hardware Installation" should be performed. After hardware installation, the segment installation can be performed following the steps described in Section 3, "Segment Installer."

- a. Plug the CT-03-92M RS-232 cable provided with the UPS software into the UPS and the computer.

NOTE: Special care should be taken to identify the cable ends labeled CPU and UPS. If cable ends are reversed the computer will power up and then start the power shutdown sequence because it can not verify the presence of the UPS.

The CPU end of the communication cable should be plugged into the TTY/A port on the SPARC computer. If this port is not available, the OnliSafe power management software will require reconfiguration as described on pages 8 through 16 of the OnliSafe Power Manual.

- b. Install the UPSI Segment using the GCCS segment installer. The only modification to the software configuration other than that noted above is related to the shutdown procedure used to shut down the system during a power outage. The default software shutdown procedures for a power outage are that the system shuts down and re-boots until power has been restored or until the UPS battery has been completely drained of power and no longer can re-boot. To modify the shutdown procedure to keep the system from attempting to re-boot:

1. Change the UPSI segment scripts directory:

```
# cd /h/COTS/UPSI/scripts
```

2. Edit the shutdown script.

```
# vi power_mon.hlt2
```

3. Edit the last line in the file to read:

```
# cd /;uadmin 2 0 > /dev/console 2>/dev/console
```

- c. After the software segment installation is completed, the system will require a system shutdown and reboot to activate the power management software.

NOTE: If the site needs further assistance, contact:

Exide Electronics
8517 Six Forks Roads
Raleigh, North Carolina 27615
(919) 870-3300

SECTION 18. EXECUTIVE MANAGER OPERATIONS

NOTE: The Executive Manager (EM) is continually being revised. Consequently the documentation in this section is a "snapshot" of the EM procedures for a particular version. There may be differences after patches are applied during the course of GCCS Version 2.1 installation.

18.1 Introduction

The System Administrator (SA) maintains control of the GCCS Desktop by providing user profiles, assigning privileges to each user, and the granting of access to system and application resources. The structure of the SA's desktop is provided in Figure 18-1.

The SA (or its designated authority, such as the Security Administrator), through the use of the Executive Manager's five programs, i.e., Security Manager, Profile Manager, Role Manager, Monitor, and Control Manager, provides the following services:

- User account maintenance: creating new accounts; modifying existing accounts; deleting existing accounts; and defining and viewing various audit logs and viewing lists of special access categories associated with users.
- System profile maintenance: adding/deleting/changing user profiles and projects.

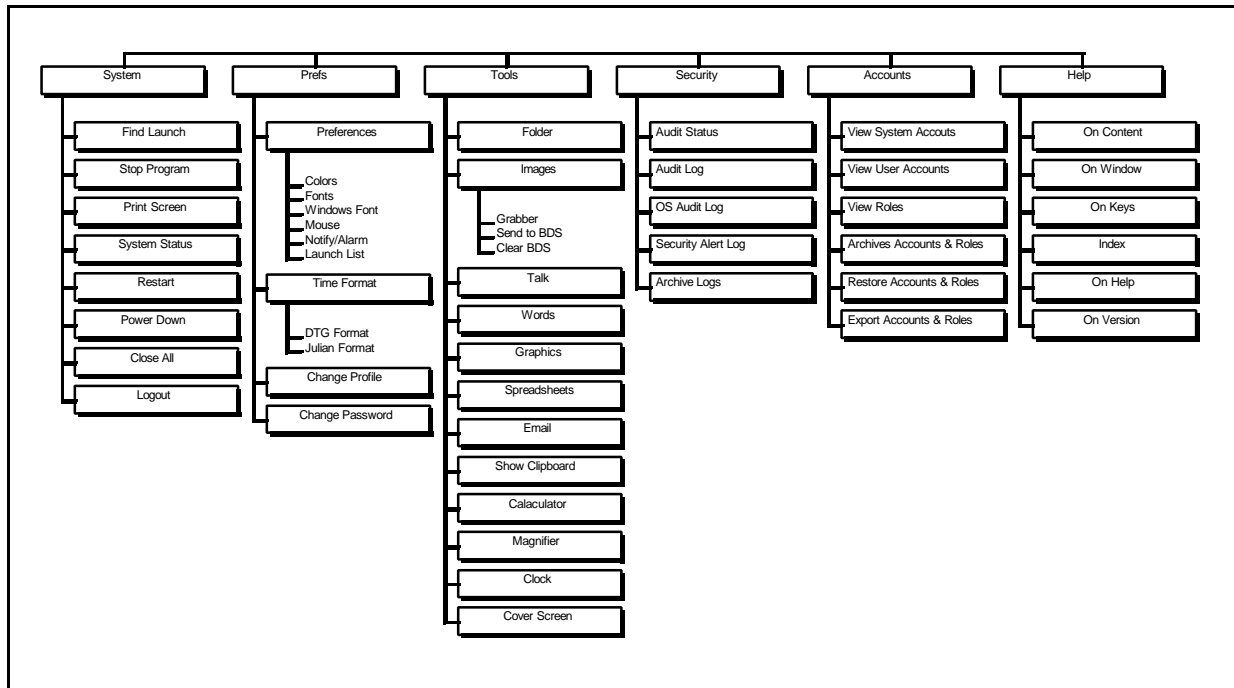


Figure 18-1. System Administrator's Desktop Menu Structure

Profiles contain information related to a user's administrative chain of command (reporting path) and permissions to access specific GCCS applications. Profile attributes consist of: Project, Position, Directorate, Division, Branch, Section, and Cell, which represent organized structures as well as folder (directory) structure access. The profile attributes have modifiers to notify the user of messages related to the user's administrative structure and folder/file handling privileges. Profiles exist only when associated with a specific user. Profiles contain a list of applications available to that specific user. That list is known as a Launch List.

Attribute modifiers are Delete rights and Notify rights. The Delete right will permit the user to delete folders and folder elements contained in the selected organization's folder. The Notify right indicates that the specific user will be informed when messages are received for that organization.

18.2 User Account Maintenance

User account maintenance is performed by the SA using the GCCS Desktop's Security Manager. (The menu structure of the Desktop's Security Manager is provided in Figure 18-2). The Security Manager is a user-interactive program that allows the SA to create new accounts, modify existing accounts, delete existing accounts, define and view various audit logs, and view lists of special-access category AMHS

messages.

Audit logs are files generated automatically by the GCCS system to save a journal of system activity performed by any user logged on to the system. There are two kinds of audit logs: UNIX logs and Database logs.

Special-access categories are specific privileges associated with the ability of a user to perform operations, create, delete, and view AMHS messages ("limdis," "exclusive," etc.)

18.2.1 Security Manager Activation. To activate the Security Manager program:

- a. Click twice in rapid succession on the **SECURITY** icon on the Session Manager's Launch Window. The "run_security" window is displayed.
- b. Enter password. Upon successful program initialization, the Security Manager main window is displayed.

18.2.2 Security Manager Termination. To exit the Security Manager:

- a. Click on **File > Exit** on the "Security Manager" menu bar. A prompt will confirm the exit request.
- b. Click on **OK**. All Security Manager-related windows vanish.

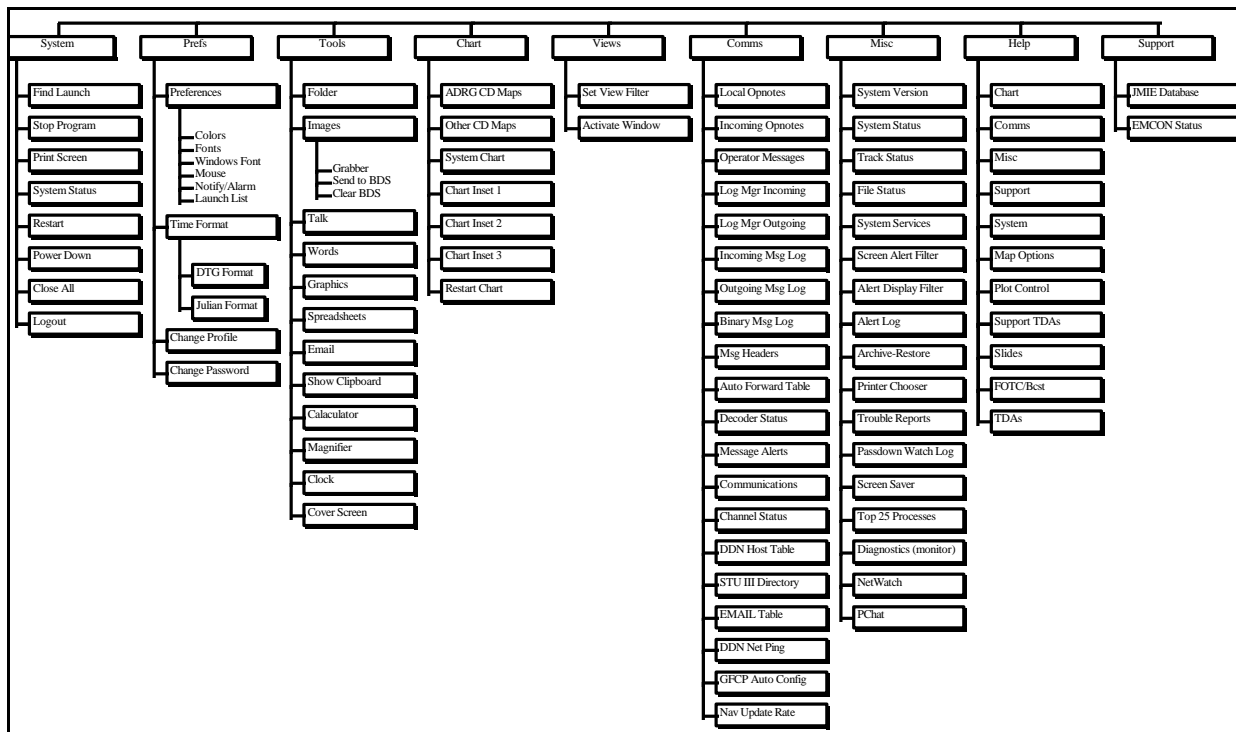


Figure 18-2. Security Manager's Desktop Menu Structure

18.2.3 Security Main Window. The Security Manager main window has the following menus on the menu bar (see Figure 18-3): "File," "Edit," "Options," and "Help." Options available in each menu are shown in Figure 18-4.

In the Security Manager main window there is listed for each account a "Userid," "Num," "D-Group," "Username," and "Group" (see Figure 18-3). D-Group represents the default group, and Group represents any other groups to which the user also retains privileges.

18.2.4 User Account Maintenance Tasks. The following paragraphs provide the necessary step-by-step actions required to utilize the capabilities provided by the Security Manager to perform user account maintenance tasks.

- a. **Creating a New Account.** To create a new user account:
 1. Activate the Security Manager, as described in paragraph 18.2.1.
 2. Click on **File > Create Account** on the "Security Manager" menu bar. The "Security Manager:Create User" window is displayed.

3. Type in all the text fields, including the Sybase System Administrator account password. The password is not visible during type-in.

Unclassified				
SECURITY MANAGER				
File	Edit	Option	Help	
<u>Userid</u>	<u>Num</u>	<u>D-Group</u>	<u>Username</u>	<u>Groups</u>
adagen			Adagen	
amargrude			Andrew margrude	
ameiding			Angela Meidinger	
amhs_dba			AMHSDBA	
barbara			barbara	
bindings			Motif Ada Bindings FTP account	
bpark			Barbara Park	
bsdirb			BSDIR	
bsj4b			BSJ4B	
carol			Carol	
ccasby			Cindi Casby	
chuck			The Penster	
clint			Clinton Miyazono	
cmiyazan			Calvin Miyazono	
dadams			Dottie Adams	
PROJECT:				

Figure 18-3. Security Manager Main Window

4. Click on the special-access categories that this user will have, then click on **Ok/Apply**. The new user account is added to the main window, in alphabetic order, with all the special access categories assigned to it. The newly created account is available for logon at this time.

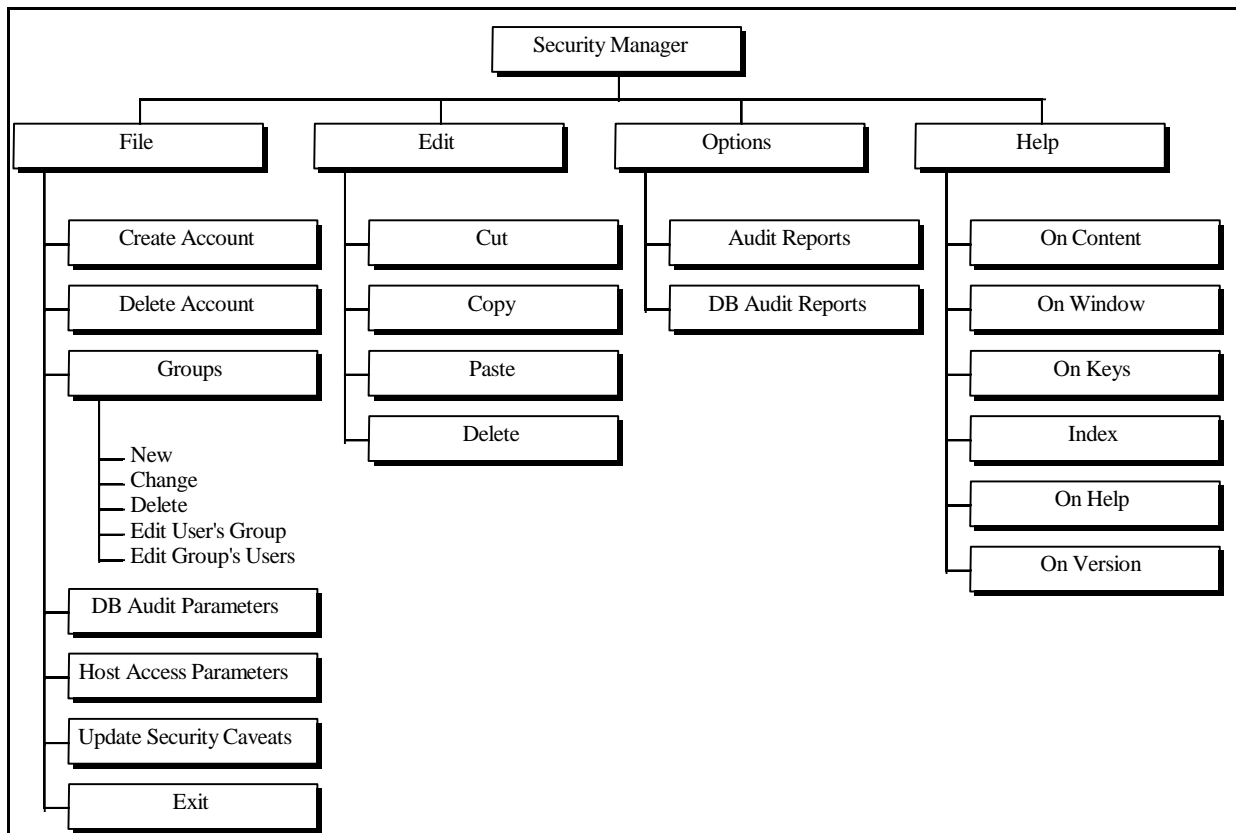


Figure 18-4. Security Manager Menu Structure

- b. **Deleting an Account.** To delete an account:
1. Click on an account to be deleted from the Security Manager main window. The selected account is highlighted.
 2. Click on **File > Delete Account** on the Security Manager menu bar. The "Security Manager:Delete Account" window is displayed.
 3. Type in the Sybase System Administrator account password. The password is not visible during type-in.
 4. Click on **yes** or **no** in response to the "Delete User Directories and Files" question.
 5. Click on **Ok/Apply**. The selected account is deleted from the main window. The duration of the delete process may vary according to the answer in step (4)

above. The deleted account is now no longer available for logon.

18.2.5 Group Maintenance Tasks. The following paragraphs provide the necessary step-by-step actions required to utilize the capabilities provided by the Security Manager to perform group maintenance tasks. The tasks are: creating a new group, deleting a group, editing user groups, and editing groups users.

y. **Creating a New Group.** To create a new group:

- (1) Activate the Security Manager as described in paragraph 18.2.1.
- (2) Click on **File > Groups > New** on the "Security Manager" menu bar. The "Security Manager: Create Group" window is displayed.
- (3) Type in all the text fields, and click on **Ok**.

z. **Changing Group.** To change a group name:

- (1) Activate the Security Manager as described in paragraph 18.2.1.
- (2) Click on **File > Groups > Change** on the "Security Manager" menu bar. The "Security Manager: Create Group" window is displayed.
- (3) Type in all the text fields and click on **Ok**.

NOTE: If a selection arrow box is to the right of a text field, clicking on the arrow will provide a list of available items. Select one and click on **Ok**; the selection is automatically entered for that field.

- (4) Rename the Group as desired. Click on **Ok**.

aa. **Deleting a Group.** To delete a group:

- (1) Activate the Security Manager as described in paragraph 18.2.1.
- (2) Click on **File > Groups > Delete** on the "Security Manager" menu bar. The "Security Manager: Delete Group" window is displayed.
- (3) Type in all the groups and click on **Ok**.

NOTE: If a selection arrow box is to the right of a text field, clicking on the arrow will provide a list of available items. Select one and click on **Ok**; the selection is automatically entered for that field.

(4) Click on **Ok**.

bb. **Editing User Groups.** To change the groups a user is associated with:

- (1) Activate the Security Manager as described in paragraph 18.2.1.
- (2) Click on **File > Groups > Edit User's Groups** on the "Security Manager" menu bar. The "Security Manager: Edit By User" window is displayed.
- (3) Type in text fields and click on **Ok**.

NOTE: If a selection arrow box is to the right of a text field, clicking on the arrow will provide a list of available items. Select one and click on **Ok**; the selection is automatically entered for that field.

- (4) This window will provide a window showing "Assigned Groups" and a window showing "Available Groups." Clicking on an item in either window will transfer that item to the opposite window, thereby either adding or deleting a group assignment for that user.
- (5) Click on **Ok**.

cc. **Editing a Group's Users.** To add or delete users within a group:

- (1) Activate the Security Manager as described in paragraph 18.2.1.
- (2) Click on **File > Groups > Change** on the "Security Manager" menu bar. The "Security Manager: Edit by Group" window is displayed.
- (3) Type in text fields and click on **Ok**.

NOTE: If a selection arrow box is to the right of a text field, clicking on the arrow will provide a list of available items. Select one and click on **Ok**; the selection is automatically entered for that field.

- (4) This window will provide a window showing "Users in Group" and a window showing "Available Users." Clicking on an item in either window, will transfer that item to the opposite window, thereby either adding or deleting a user in a group.
- (5) Click on **Ok**.

18.2.6 Audit Monitoring. This capability allows the SA to obtain UNIX audit logs and GCCS Desktop Database audit logs.

18.2.6.1 Setting DB Audit Parameters. This capability allows the SA to set the operating parameters for the GCCS Desktop database audit daemon. The setting of parameters entails selecting table operation(s) to be audited on the GCCS Desktop database tables, and audits of login and logoff attempts. To set DB Audit Parameters:

- a. Click on **File > DB Audit Parameters** on the Security Manager menu bar. The "Security Manager:Database Audit Parameters" window is displayed. Note that the window contains a list of all the GCCS Desktop database tables and operations representing the various audit operations.
- b. Click on the user for whom the audit parameters are to be set.
- c. Click on the table name for the audit parameters to be set. The name of the selected table is highlighted.
- d. Click on any combination of operations—Retrieve, Update, Insert, Delete—in the "Security Manager:Database Audit Parameters" window. As each of the operations is selected, the first letter of the operation appears in the Code column corresponding to the selected table name in Step c above.
- e. Click on **Auditing Off** in the "Security Manager:Database Audit Parameters" window. The button label changes to "Auditing On." This is a required step if auditing of database operations is desired. Note that the default is "Auditing Off."
- f. If auditing of logins is desired, click on **Logins Off** in the "Security Manager:Database Audit Parameters" window. The

button label changes to "Logins On." Note that the default is "Logoffs Off."

- g. Click on **Reset** in the "Security Manager:Database Audit Parameters" window if all the selections made in steps b through f are to be cancelled.
- h. Click on **Apply** in the "Security Manager:Database Audit Parameters" window if all the selections made in steps b through f are to be saved. An audit trail will be available to view through "Option > Unix Audit Logs," and "Option Database Audit Logs" on the Security Manager menu bar.

18.2.6.2 Viewing UNIX Audit Logs. This option allows the SA, with default to the last 24 hours, to display a UNIX system log for each of the following (one at a time): All Logins, Failed Logins, Privileged Commands, and Unauthorized Access. To obtain a UNIX audit log display, do the following:

- A. Click on **Option > Audit Reports** on the Security Manager menu bar. The "Security Manager:Unix Audit Display" window is displayed. Note that the period of audit is the last 24 hours.
- B. Click on the type of audit log to be displayed by clicking on one of the following options:
 - All Logins
 - Failed Logins
 - Privileged Commands
 - Unauthorized Access.
- C. Click on **Display** in the "Security Audit Reports" window. The selected, audit log type in step b is displayed.
- D. Repeat steps b and c for each audit log type.

18.2.6.3 Viewing Database Audit Logs. This option allows the SA, with default to the last 24 hours, to obtain a GCCS Desktop Database log. The log contains the date, event, user name and pass/fail indication for the event. To obtain a GCCS Desktop database audit log:

- A. Click on **Option > Database Audit Reports** on the Security Manager menu bar. The "Security Manager:DB Audit Display" window is displayed. Note that the period of audit is the last 24 hours.
- B. Set the correct audit period within the "From Dtg" and "To Dtg" areas and click on Display in the "Security Manager:Database Audit Display" window. The log containing the audit trail is displayed.

- C. Click on Print in the "Security Manager: Database Audit Display" window if a printout of the audit log is desired.

18.2.7 Updating Security Caveats. This capability allows the SA to update the security caveats list by adding new or deleting existing security caveats. To update the security caveats list:

- A. Click on **File > Update Security Caveats** on the "Security Manager" menu bar. The "Security Manager-Update Security Caveats" window is displayed.
 - 1. To add a caveat:
 - a. Type in the name of the new caveat in the Caveat Name text area in the bottom of the "Security Manager:Edit Caveats."
 - b. Click on **Add** in the "Security Manager:Edit Caveats" window. The new caveat name is added to the end of the existing list.
 - 2. To delete a caveat:
 - a. Click on the name of the caveat, in the existing list, to be deleted. The selected name is highlighted and it appears in the Caveat Name text area in the bottom of the "Security Manager:Edit Caveats" window.
 - b. Click on **Delete** in the "Security Manager-Edit Caveats" window. The selected caveat name disappears from the existing caveats list.

18.2.8 Setting Access Parameters. This capability allows the SA to set or view host processors available to GCCS at a particular site. To set or view host access:

- A. Click on **File > Host Access Parameters** on the Security Manager menu bar. The "Security Manager:Host Access Parameters [GCCS]" window is displayed. Note that the window consists of a list of hosts available and a host access list.
- B. Click on **File > Open Access File** in the "Security Manager:Host Access Parameters [GCCS]" window.
- C. Select the GCCS platform containing the desired file.
- D. Click on **Apply** in the "Security Manager:Open Access File" window.

- E. Click the desired host on the "Host Available List" to select a host.
- F. Click in the Host Access List to choose specific access parameters.

18.3 System Profile Maintenance

System Profile Maintenance is performed by the SA using the GCCS Desktop Profile Manager. The Profile Manager is an interactive program that is used to manage user profile information. This program resides on the GCCS Desktop Dedicated Processor and is started via the Session Manager launch window. The Profile Manager performs the following functions:

- Creates/modifies/deletes profile attributes
- Creates/modifies/deletes new user profiles
- Modifies user's Launch List
- Displays existing users based on profiles.

18.3.1 Profile Description. The construction of a profile for a particular user requires certain profile attributes to be available for (or created prior to) insertion into a profile. These attributes are Project, Position, Directorate (optional), Divisions (optional), Branch (optional), Section (optional), and Cell (optional). If the optional attributes exist, they must also be included.

18.3.1.1 Profile Manager Activation. Click twice in rapid succession on the **PROFILE** icon on the Session Manager's launch window. Upon successful program initialization, the Profile Manager main window is displayed, as shown in Figure 18-5.

Currently Selected Profiles					
1*					
No	User Id	: 1024 Id:	Lloyd DeForrest		
	deforres Name:				
Name	Project	: Demo Storm	Project Notify	: NOTIFY	DELETE
	Position	: BSDIR	Position Notify	: Notify	DELETE
		: ECJ1	Directorate	:	DELETE
Directorate	Directorate		Notify	NOT_NOTIFY	
	Division	: Force Integration	Division Notify	:	NOT_NOTIFY
	Branch	: Admin Branch	Branch Notify	:	NOT_NOTIFY
	Section	: Ops Briefing/Graphics	Section Notify	:	NOT_NOTIFY
	Cell	: JSE	Cell Notify	:	NOT_NOTIFY
2					
No	User Id	: 1024 Id:	Lloyd DeForrest		
	deforres Name:				
Name	Project	: Day to Day Operations	Project Notify	:	NOT_NOTIFY
	Position	: USER	Position Notify	:	NOT_NOTIFY
		: ECJ3	Directorate	:	NOT_NOTIFY
Directorate	Directorate		Notify	NOT_NOTIFY	
	Division	: Division 437	Division Notify	:	NOT_NOTIFY
	Branch	: Admin Branch	Branch Notify	:	NOT_NOTIFY
	Section	: Ops Briefing/Graphics	Section Notify	:	NOT_NOTIFY
	Cell	: JSE	Cell Notify	:	NOT_NOTIFY
	Userid	: deforres Lloyd DeForrest	Branch	:	_
	Project	:	Section	:	_
		:	Cell	:	_
Directorate					
	Division	:	Position	:	_
<div> <div>Update Profile Filter</div> <div>Clear Profile Filter</div> </div>					
PROJECT: Not Applicable					

Figure 18-5. Profile Manager Main Window

18.3.1.2 Profile Manager Termination. To exit the Profile Manager computer program:

- A. Click on **File > Exit** on the "Profile Manager" menu bar. You will be prompted to confirm the exit request.
- B. Click on **OK**. All Profile Manager-related windows vanish.

18.3.2 Profile Manager Menus. The Profile Manager has five menus: File, Edit, Options, Modify, and Help. Choices available in these menus are illustrated in Figure 18-6.

The Profile Manager main window (Figure 18-5) contains two distinct areas: the top portion of the window is where selected profiles are displayed, the bottom is used as a filter.

Also included in this display are the organization "Notify" and "Delete Rights" indicators. When the Notify indicator displays "NOTIFY" next to an organization, the user will be notified when messages are received for that organization. The Delete Rights indicator displays "DELETE," to indicate the user has been given Delete Rights to elements in that organization's folder.

18.3.3 System Profile Maintenance Tasks. The following paragraphs provide the necessary step-by-step actions required to utilize the capabilities provided by the Profile Manager computer program.

18.3.3.1 Viewing Users and Profiles. Upon successful program initialization the Profile Manager main window is displayed.

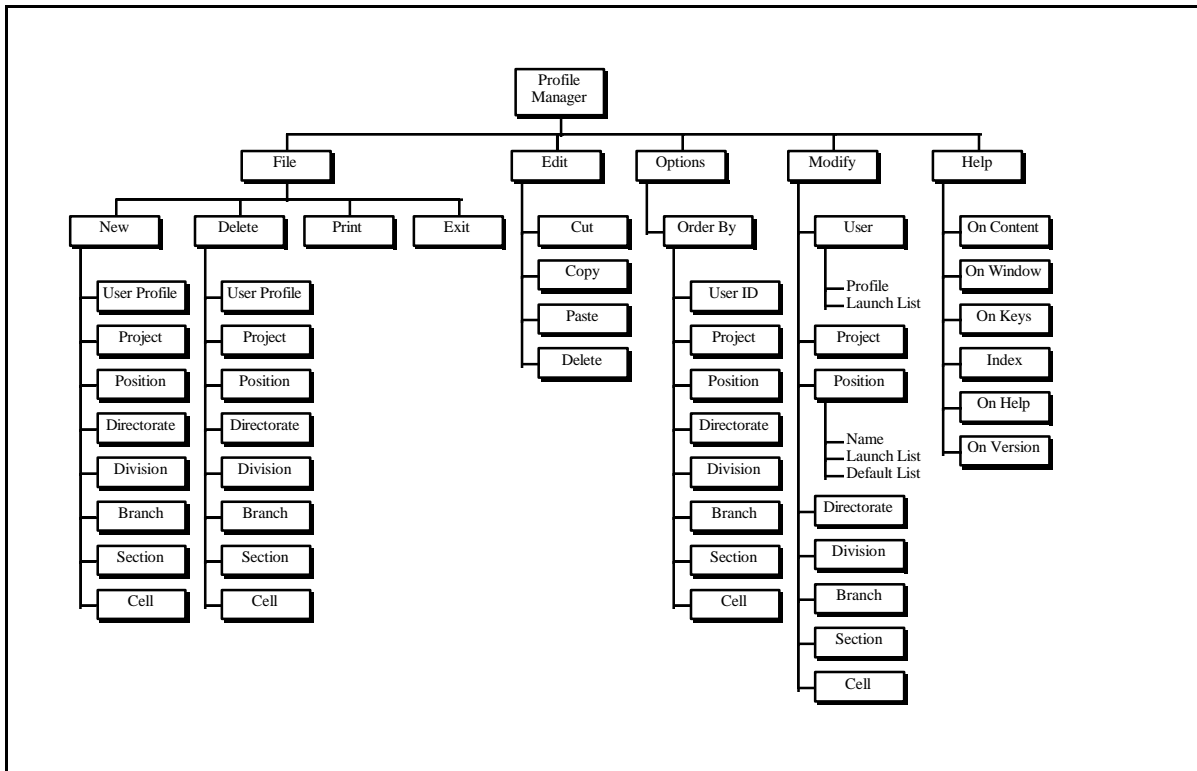


Figure 18-6. Profile Manager Menu Structure

The user profiles displayed in the main window can be filtered according to criteria listed in the bottom of the main window. Each of the filter criteria is selected from a pop-up selection list. For example: selecting user ID alone will show all profiles for a particular user, while selecting any other profile attributes without the user ID will show all users with the chosen profile attributes. To display profile(s) that correspond to a certain filter criterion:

- A. Click on a pop-up selection button for profile attributes to be used for the profiles to be listed. The pop-up selection dialog for the selected profile attribute is displayed.
 1. Click on the name of the selection to be used for this profile attribute.
 2. Click on **Ok/Apply**. The selected name appears in the corresponding profile attribute text field in the main window. Click on **Undo** in the pop-up selection dialog if a selection is to be changed. The last selection will be removed from the main window. Note that the "Update Profile Filter" and "Clear Profile Filter" buttons in the bottom of the main window become active after the first filter profile attribute is entered

(these buttons are initially stippled).

- B. Repeat step a above for each profile attribute desired.
- C. Click on **Update Profile Filter** button on the main window. All user profiles that meet the filter criteria are displayed in the main window with the default profile being marked by an asterisk (*).
- D. Click on **Clear Profile Filter** to erase all filter criteria previously selected, and the profiles displayed in the main window. This action results in the "Update Profile Filter" and the "Clear Profile Filter" buttons becoming stippled again.

18.3.3.2 Profile Attribute Maintenance. The attributes that make up the components of a profile are Project, Position, Directorate, Divisions, Branch, Section, and Cell. Some attributes are optional; however, if they are used in a profile, they must have been previously created. While each attribute is created/deleted/modified separately, relationships also exist between some of the attributes that require cross-checking when an attribute is worked on, specifically between Project and Positions, and Project and Cell. The following list describes all attributes:

- **Project.** A project represents one of the GCCS activities that have been defined for a particular facility or facilities in which GCCS is operating. This attribute must be specified when creating a user profile.
- **Position.** This attribute represents a specific task or assignment undertaken by a user. Positions belong to one or more projects; therefore a project name must be selected during the creation of a position.
- **Directorate.** This is an optional attribute.
- **Division.** This is an optional attribute.
- **Branch.** This is an optional attribute.
- **Section.** This is an optional attribute.
- **Cell.** All cells belong to a project, therefore a project name must be selected during creation of a cell. "Cell" is an optional attribute.

- A. **Creating a new project.** To create a new project:
 - 1. Click on **File > New > Project** on the Profile Manager menu bar. The "Add New Project" dialog is displayed.
 - 2. Type in the name of the new project (maximum of 25 characters; no special characters are allowed). If the "Default Positions" list is to be used with this new project, click on the **Use Default Positions** button

in the "Add New Project" dialog.

3. Click on **Ok/Apply** to save the new project name.

NOTE: For every project created, there must be an associated position. Validation of the project/position pair must be manually performed off-line prior to insertion into a user profile.

B. Creating a New Position. To create a new position:

1. Click on **File > New > Position** on the Profile Manager menu bar. The "Add a New Position" dialog is displayed.
2. Since all positions belong to a project, select a project name via the pop-up selection button.
3. Type in the name of the new position (maximum of 8 characters; no special characters are allowed).
4. Type in a description of the position name (maximum of 25 characters).
5. Click on **Ok/Apply** to save the new position name.

NOTE: For every project created, there must be an associated position. Validation of the Project/Position pair must be manually performed off-line prior to insertion into a user profile.

C. Creating a New Directorate. To create a new directorate:

1. Click on **File > New > Directorate** on the Profile Manager menu bar. The "Add a New Directorate" dialog is displayed.
2. Type in the name of the new directorate (maximum of 25 characters).
3. Click on **Ok/Apply** to save the new directorate name.

D. Creating a New Division. To create a new division:

1. Click on **File > New > Division** on the Profile Manager menu bar. The "Add a New Division" dialog is displayed.
2. Type in the name of the new division (maximum of 25 characters).

3. Click on **Ok/Apply** to save the new division name.

E. **Creating a New Branch.** To create a new branch:

1. Click on **File > New > Branch** on the Profile Manager menu bar. The "Add a New Branch" dialog is displayed.
2. Type in the name of the new branch (maximum of 25 characters).
3. Click on **Ok/Apply** to save the new branch name.

F. **Creating a New Section.** To create a new section:

1. Click on **File > New > Section** on the Profile Manager menu bar. The "Add a New Section" dialog is displayed.
2. Type in the name of the new section (maximum of 25 characters).
3. Click on **Ok/Apply** to save the new section name.

G. **Creating a New Cell.** To create a new cell:

1. Click on **File > New > Cell** on the Profile Manager menu bar. The "Add New Cell" dialog is displayed.
2. Since all cells belong to a project, select a project name via the pop-up selection button.
3. Type in the name of the new cell (maximum of 25 characters).
4. Click on **Ok/Apply** to save the new cell name.

H. **Deleting a Project.** To delete a project:

1. Click on **File > Delete > Project** on the Profile Manager menu bar. The "Delete an Existing Project" dialog is displayed. Note the warning that all profiles assigned to this project will be deleted.
2. Select the project to be deleted via the pop-up selection button.
3. Click on **Ok/Apply** to delete the selected project name.

I. **Deleting a Position.** To delete a position:

1. Click on **File > Delete > Position** on the Profile Manager menu bar. The "Delete an Existing Position" dialog is displayed.
 2. Select a project name via the pop-up selection button.
 3. Select a position name via the pop-up selection button.
 4. Click on **Ok/Apply** to delete the selected position name.
- J. **Deleting a Directorate.** To delete a directorate:
1. Click on **File > Delete > Directorate** on the Profile Manager menu bar. The "Delete an Existing Directorate" dialog is displayed. Note the warning that all profiles assigned to this directorate will be deleted.
 2. Select a directorate name via the pop-up selection button.
 3. Click on **Ok/Apply** to delete the selected directorate name.
- K. **Deleting a Division.** To delete a division:
1. Click on **File > Delete > Division** on the Profile Manager menu bar. The "Delete an Existing Division" dialog is displayed. Note the warning that all profiles assigned to this division will be deleted.
 2. Select a division name via the pop-up selection button.
- L. **Deleting a Branch.** To delete a branch:
1. Click on **File > Delete > Branch** on the Profile Manager menu bar. The "Delete an Existing Branch" dialog is displayed. Note the warning that all profiles assigned to this branch will be deleted.
 2. Select a branch name via the pop-up selection button.
 3. Click on **Ok/Apply** to delete the selected Branch name.
- M. **Deleting a Section.** To delete a section:

1. Click on **File > Delete > Section** on the Profile Manager menu bar. The "Delete an Existing Section" dialog is displayed. Note the warning that profiles assigned to this section will be deleted.
2. Select a section name via the pop-up selection button.
3. Click on **Ok/Apply** to delete the selected section name.

N. Deleting a Cell. To delete a cell:

1. Click on **File > Delete > Cell** on the Profile Manager menu bar. The "Delete an Existing Cell" dialog is displayed.
2. Select a project name via the pop-up selection button.
3. Select a cell name via the pop-up selection button.
4. Click on **Ok/Apply** to delete the selected cell name.

O. Modifying a Project. To modify a project:

1. Click on **Modify > Project** on the Profile Manager menu bar. The "Modify Existing Project" dialog is displayed.
2. Select the project name to be modified via the pop-up selection button.
3. Type in the new project name (maximum of 25 characters; no special characters are allowed).
4. Click on **Ok/Apply** to modify the selected project name.

P. Modifying a Position. Position modification entails the following: modifying the name of a position within a project, modifying the list of launch buttons assigned to a position, and modifying the default list of positions assigned to a new project.

1. To modify a position name within a project:
 - a. Click on **Modify > Position > Name** on the Profile Manager menu bar. The "Modify an Existing Position" dialog is displayed.
 - b. Select the project name via the pop-up selection button.

- c. Select the old position name via the pop-up selection button.
 - d. Type in the new position name (maximum 8 characters; no special characters are allowed).
 - e. Click on **Ok/Apply** to modify the selected old position name.
2. To modify a position launch button list:
 - a. Click on **Modify > Position > Launch List** on the Profile Manager menu bar. The "Edit Position Launch List" dialog is displayed.
 - b. Select the position name via the pop-up selection button. A list of all available launch buttons is displayed in the right side of the "Edit Position Launch List" dialog. On the left side are all the launch buttons currently assigned to the selected position. Click on a name in one list to move it to the other.
 - c. Click on **Ok** to save the assigned launch button list.
3. To modify a position default list:
 - a. Click on **Modify > Position > Default List** on the Profile Manager menu bar. The "Edit Default Position List" dialog is displayed. The list of commonly used positions is displayed in the right side of the "Edit Default Position List" dialog. On the left side are all the default positions. Click on a name in one list to move it to the other. This default list is not GCCS-related. This data was used for UCOM. Do not use this option until further notice.
 - b. Click on **Ok/Apply** to modify the default list.
- Q. **Modifying a Directorate.** To modify a directorate:
 1. Click on **Modify > Directorate** on the Profile Manager menu bar. The "Modify Existing Directorate" dialog is displayed.
 2. Select an old directorate name via the pop-up selection button.
 3. Type in the new directorate name (maximum of 25 characters)

4. Click on **Ok/Apply** to modify the selected directorate name.

R. **Modifying a Division.** To modify a division:

1. Click on **Modify > Division** on the Profile Manager menu bar. The "Modify Existing Division" dialog is displayed.
2. Select an old division name via the pop-up selection button.
3. Type in the new division name (maximum of 25 characters).
4. Click on **Ok/Apply** to modify the selected division name.

S. **Modifying a Branch.** To modify a branch:

1. Click on **Modify > Branch** on the Profile Manager menu bar. The "Modify Existing Branch" dialog is displayed.
2. Select an old branch name via the pop-up selection button.
3. Type in the new branch name (maximum of 25 characters).
4. Click on **Ok/Apply** to modify the selected branch name.

T. **Modifying a Section.** To modify a section:

1. Click on **Modify > Section** on the Profile Manager menu bar. The "Modify Existing Section" dialog is displayed.
2. Select an old section name via the pop-up selection button.
3. Type in the new section name (maximum of 25 characters).
4. Click on **Ok/Apply** to modify the selected section name.

U. **Modifying a Cell.** To modify a cell:

1. Click on **Modify > Cell** on the Profile Manager menu bar. The "Modify Existing Cell" dialog is displayed.

2. Select a project name via the pop-up selection button.
3. Select an old cell name via the pop-up selection button.
4. Type in the new cell name (maximum of 25 characters).
5. Click on **Ok/Apply** to modify the selected cell name.

18.3.4 User Profile Maintenance. Every entry into this window is done via a pop-up selection dialog and it is here that the Delete Rights can be set for each entry. The mandatory entries are User ID, Project Name, and Position Name.

Additionally, before a position name and/or cell name can be selected, a project name must first be selected.

18.3.4.1 Creating a New User Profile. To create a new user profile:

- A. Click on **File > New > User Profile** on the Profile Manager menu bar. The "Add a New User Profile" window is displayed.
 1. Click on the pop-up selection dialog buttons for those fields chosen to become part of the user profile.
 2. Select the **Grant Delete Rights** button if the user will have the right to delete folders and folder elements contained in the selected organization's folder. The user is granted delete rights if the "Grant Delete Rights" button is pushed in (button shaded).
- B. Click on **Ok/Apply**. The entries are then verified, and if valid, the new user profile is added into the system.

18.3.4.2 Delete a User Profile. To delete a user profile:

- A. Display the profile to be deleted in the main window, and click anywhere within this profile.
- B. Click on **File > Delete > User Profile** on the Profile Manager menu bar. The "Delete User Profile" window containing the selected profile is displayed.
- C. Click on **Ok/Apply**. The selected profile is deleted and is not recoverable.

18.3.4.3 Modifying a User Profile. To modify a user profile:

- A. Display the profile to be modified in the main window, and

click anywhere within this profile.

- B. Click on **Modify > User > Profile** on the Profile Manager menu bar. The "Modify an Existing User Profile" window is displayed containing the selected profile for modification. All entries, except User ID, can be modified via pop-up selection buttons.
- C. Make all modifications.
- D. Click on **Ok/Apply**. The selected profile is modified as per Step c.

18.3.5 Launch List Maintenance. When a profile is assigned to a user by the SA, specific application access or privileges are also assigned. When the users logs on, a window on the GCCS Desktop displays a set of icons that represent the applications available to the user. This is known as a launch window. The SA populates that window by choosing specific applications from the applications in the Available Launch List and inserting them into the user's launch list. The Available Launch List contains all available applications that have been properly installed through the use of the System Installer.

18.3.5.1 Modifying a User Launch List. To modify a user launch list:

- A. Click on **Modify > User > Launch List** on the Profile Manager menu bar. The "Edit User Launch List" window is displayed.
- B. Select a User ID via the pop-up selection button. All launch buttons available are listed in the right side of the "Edit User Launch List." The left side contains the launch buttons that are assigned to the User ID selected. Click on the right side name to move it to the left side, or click on the left side to move it to the right side.
- C. Click on **OK** to save a user launch list.

18.3.6 Profiles Display Order. Once profiles are displayed in the Currently Displayed Profiles area of the main window, the SA has the ability to change the order in which they are displayed. The default ordering is by User ID. Profiles can be ordered (in alphabetical order) according to the following eight criteria: User ID, Project, Position, Directorate, Division, Branch, Section, and Cell.

To order the profiles listed according to a specific criterion:

- A. Click on **Options > Order By > <a criterion>**, where <a criterion> is one of the eight criteria listed above. After a short time, the Currently Selected Profiles display in the main window is updated to reflect the order according to the criterion selected. The sort order is as follows: Blanks,

Numbers, UPPER CASE LETTERS, and lower case letters.

18.4 System Assign Roles Maintenance

System Assign Roles Maintenance is performed by the SA using the GCCS Desktop Role Manager. The Role Manager is an interactive program that is used to assign roles to users, such as: Security Administrator, System Administrator, and GCCS Operator. This program resides on the GCCS Desktop Dedicated Processor and is started via the Session Manager launch window. The profile performs the following functions:

- Assigns roles to specified account groups by User IDs.
- Deletes roles from specified account groups by User IDs.
- Edits roles to specified account groups by User IDs.
- Duplicates roles of account groups to allow the SA to revise previously entered data to avoid repetitive entry when creating additional roles.
- Print the assigned role of a user.

18.4.1 Role Manager Activation. To activate the Role Manager program, execute the following:

- A. Enter **USERNAME: SECMAN** [RETURN]
Enter **PASSWORD** [RETURN]
- B. Click twice in rapid succession on the **ROLE** icon on the Session Manager's launch window. Upon successful program initialization the Role Manager main window is displayed, as shown in Figure 18-7.

ROLE		ACCT GROUP	CLASSIFICATION		
GCCS Default		GCCS Operator	xxxxxxxxxxx		
SA Default		System Admin	xxxxxxxxxxx		
SSO Default		Security Admin	xxxxxxxxxxx		
ADD	DELETE	EDIT	DUPLICATE	PRINT	
EXIT					

Figure 18-7. Role Manager Main Window

18.4.2 Role Manager Termination. To exit the Role Manager, execute the following:

- A. Click on **File>Exit** on the Role Manager menu bar. You will be prompted to confirm the exit request.
- B. Click on **Ok**. All Role Manager-related windows vanish.

18.4.3 Role Manager Menus. The Role Manager allows the user to add roles to applicable account groups. The structure is shown in Figure 18-8.

18.4.4 Adding a Role to Account Group: Security Admin

- A. Click on **Add** in the Role Manager main window (Figure 18-7). The Add Role main menu will appear (see Figure 18-9).
- B. Enter name.
- C. Enter security.
- D. Select **Security Admin** Account Group and click on **OK**.
- E. The Security Admin Role Header window will be displayed (see Figure 18-10).
- F. To grant permissions to the role, click on the desired permissions in the Permission list in the Security Admin Role Header window, and click **Add**.

Each permission will have a separate screen to enter applicable data.

- G. Click on **Edit** only if any one of the permissions needs to be modified.
- H. Click on **Menu Access** only if the Security Administrator needs to access the menu for Accounts or Security. Refer to Figure 18-8 to view the structure.

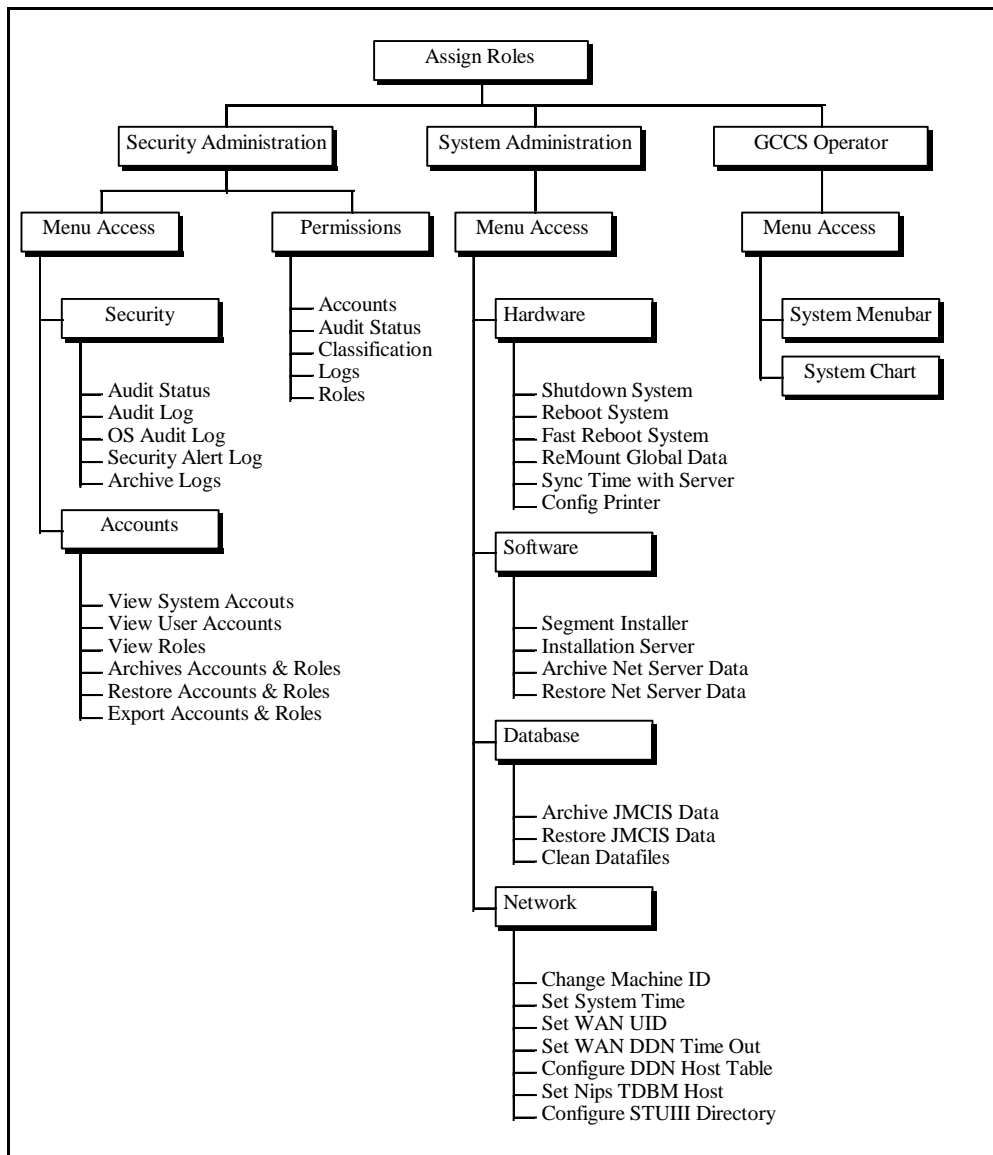


Figure 18-8. Role Manager Menu Structure (Part 1 of 3)

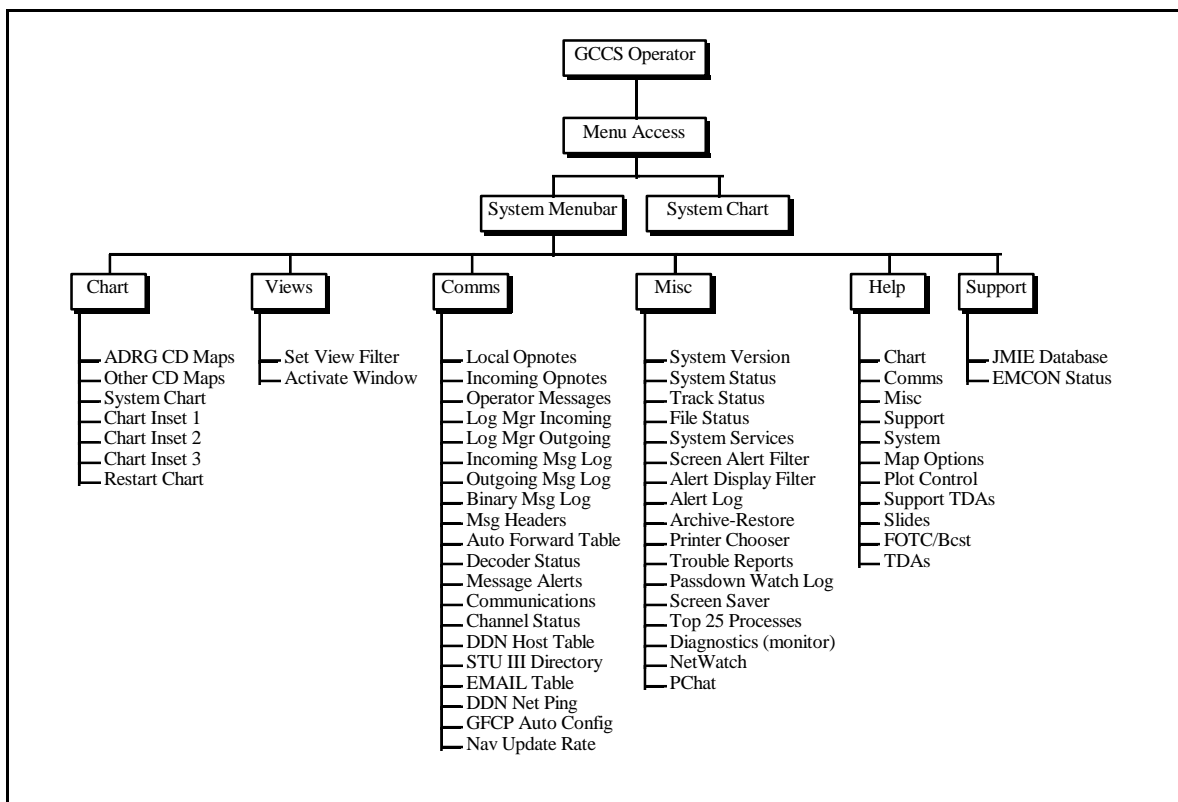


Figure 18-8. Role Manager Menu Structure (Part 2 of 3)

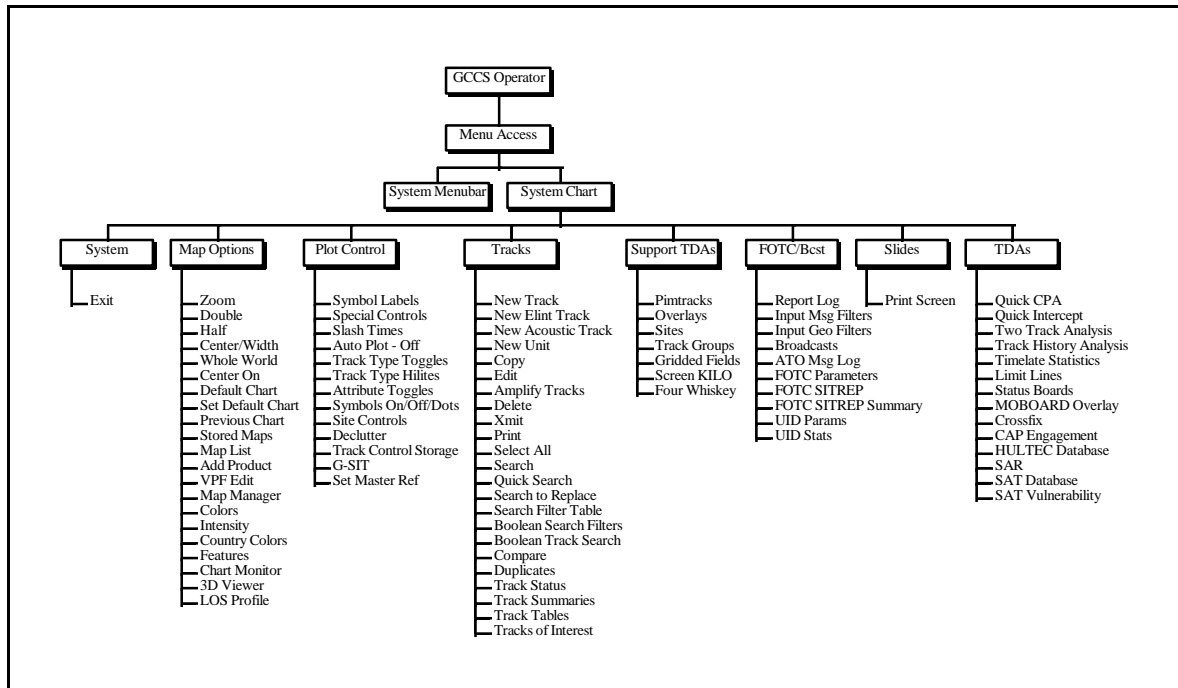


Figure 18-8. Role Manager Menu Structure (Part 3 of 3)

NAME
SECURITY
ACCOUNT GROUPS	
Security Admin	
System Admin	
GCCS Operator	
CANCEL	OK

Figure 18-9. Add Role Main Menu

ROLE HEADER			
NAME:		
ACCT GROUP:		
SECURITY:		
PERMISSIONS			
Accounts			
Audit Status			
Classification			
Logs			
Roles			
A:Add	D>Delete	E>Edit	P: Pr in t
R:Restore	V:Archive	X:Export	
EDIT MENU ACCESS Sec Admin			
CANCEL			OK

Figure 18-10. Security Admin Role Header

18.4.5 Adding a Role to Account Group: System Admin

- Return to the Add Role main menu (Figure 18-9). Select **System Admin** Account Group and click on **OK**. This will bring up the System Admin Account Group window (see Figure 18-11).
- Enter name.
- Enter account group.
- Enter security.
- Click on **Menu Access** only if the System Administrator needs to access the menu for Hardware, Software, Database, or Network options. Refer to Figure 18-8 to view the structure.

NAME:
ACCT GROUP:	System Admin
SECURITY:
MENU ACCESS	
System Admin	
CANCEL	OK

Figure 18-11. System Admin Account Group

18.4.6 Adding a Role to Account Group: GCCS Operator

- Return to the Add Role main menu (Figure 18-9). Select **GCCS Operator** Account Group and click on **OK** (see Figure 18-12).
- Enter name.
- Enter account group.
- Enter security.
- Click on **Menu Access** only if the SA needs to access the System Menu Bar Options or System Chart Options. Refer to Figure 18-8 to view the structure.

NAME:
ACCT GROUP:	GCCS Operator
SECURITY:
MENU ACCESS	
System Menubar	System Chart
CANCEL	OK

Figure 18-12. GCCS Operator Account Group

18.4.7 Deleting a Role from an Account Group

- In the Role Manager main window (Figure 18-7), click on **Delete** to allow the SA to delete an existing user. A confirmation window will be given.

18.4.8 Edit an Existing Role for an Account Group

- In the Role Manager main window (Figure 18-7), click on **Edit**

to allow the SA to modify an existing user.

18.4.9 Duplicate a Role from an Existing User

- A. In the Role Manager main window (Figure 18-7), click on **Duplicate** to allow the user to duplicate SA information in order to create another new user.

18.4.10 Print a Role of a User(s)

- A. In the Role Manager main window (Figure 18-7), click on **Print** to invoke the JMCIS printer.

18.4.11 Exit the Role Manager Main Menu

- A. In the Role manager main window (Figure 18-7), click on **Exit** to return to the Desktop.

18.5 The Monitor Program

The Monitor launch button runs the Monitor program. This program, under the Options menu (Figure 18.13) presents several useful displays for monitoring the various logs, alarms, and reports.

18.6 The Control Manager Program

The Control Manager launch button contains the **Startup**, **Shutdown**, and other options for selectable hosts. Figure 18-14 presents the menus for the Control Manager. Under the Control menu are the various options. Selection of the **Startup** and **Shutdown** options brings up a window where in the server and host to be started or shut down are selected. Clicking on the **Apply** button executes the command for the selected machines.

Selecting the **Kill** and **Initialize** options brings up a window with the list of servers. Highlighting the server and clicking the **Apply** button will execute the selected command for that server.

Selecting the **Execute** option presents a list of hosts and a command input window.

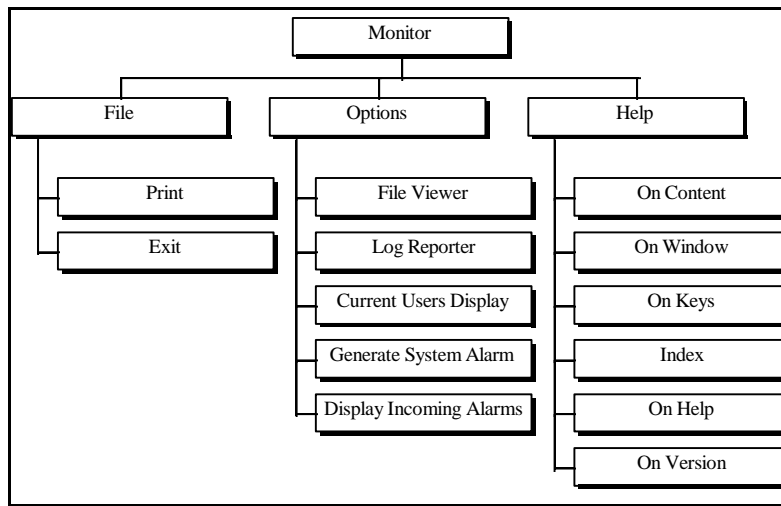


Figure 18-13. Monitor Menu

Selecting the **Report** option currently presents five command options and the host list. The command options are:

- Audit Log
- DEC Processor Status
- Executable List
- Local Password File
- Mac Spt File.

The Local Password File command will cause the password file from the selected host (not the `/etc/shadow` file) to open for scrolling perusal.

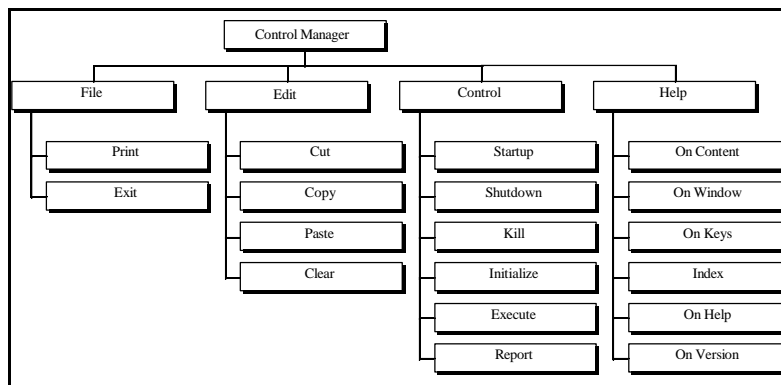


Figure 18-14. Control Manager Menu

SECTION 19. ANSWERBOOK ADMINISTRATION

The procedures in this section assume you have a CD drive installed locally (connected to your system).

NOTE: After adding a local CD-ROM drive to a Solaris 2.3 system, type **init 0** to halt the system. Then type **boot -r** from the ok PROM prompt to reconfigure the device drivers so that the system can access the CD drive. If the > PROM prompt is displayed, type **n** to display the ok PROM prompt.

- a. Insert (mount) the CD-ROM:
 1. Place the AnswerBook CD-ROM into the caddy, if a caddy is used.
 2. Insert the CD-ROM into the drive.

NOTE: If the volume management daemon is enabled (the default with Solaris 2.3), inserting the CD will mount it automatically. If you have disabled volume management, mount the CD using the **mount (1M)** command.

File Manager will now open, displaying the contents of the CD-ROM.

- b. Begin the installation with *pkgadd*:
 1. Become superuser:

su -
 2. Run *pkgadd* to begin the installation.

pkgadd -d /cdrom/cdrom0

The path shown in the example is the mount point if volume management is enabled (the default with Solaris 2.3). If you have disabled volume management, make sure the path you specify is the correct mount point for the CD.

The installation software presents a numbered list of all the packages on the disk and their associated AnswerBook titles, and will prompt you for a selection.

For example:

- 1 SUNWabc ABC AnswerBook (pltfrm) 1.2.1
- 2 SUNWabook Another AnswerBook (pltfrm) 40.5.2
- 3 SUNWasys System AnswerBook (pltfrm) 78.9.3

Select package(s) you wish to process (or 'all' to process all packages). (Default: all) [?,??,q]:

3. Specify one or all AnswerBook packages you want to install.

The default is all. Press <return> to accept the default or type **all**. Each AnswerBook package will be installed successively, and prior to each package installation you will be prompted for information.

Alternatively, you can install a single AnswerBook package by typing its number from the list.

NOTE: If you want to install all the packages on the disk, but you're concerned about available disk space, you can determine the *approximate* size of the contents of the CD-ROM this way:

- (a) Change to the CD-ROM directory.

```
# cd /cdrom/cdrom0
```

- (b) List the size of the individual packages contained on the CD:

```
# du -k .
```

Do a rough calculation of the sum of the package sizes you see listed to get an idea of how much disk space you'll need when you install.

- c. Review installation options:

For each AnswerBook package you install, you will be asked to choose an installation option:

Copyright information....

The installation options are as follows:

Option: Description:

1. nil: less than X Megabyte disk space required [slowest performance].
2. heavy: XX Megabytes disk space required [best performance].

Enter the number of an installation option from the list above (1 or 2).

Make sure to choose a parent directory on a file system big enough to accommodate all the files to

be moved for the INSTALL OPTION you selected.

The table below explains more about these install options.

Table 19-1. AnswerBook Installation Options

Required Disk Space Option	Description	(Mbytes)	Install Time
nil	Leaves almost all files on CD-ROM. Saves disk space but requires that the AnswerBook CD remain in the drive, dedicated to AnswerBook use.	<1	<5 min.
heavy	Stores all files on hard disk. Optimizes <15-30 min. AnswerBook performance. This with the configuration is recommended if the package, AnswerBook package is to be shared from by multiple systems and users under 1 up to 50 or more	Varies	

To check the amount of available disk space on your system, see Step d.
Otherwise, skip to
Step e.

- d. Check the space available for the AnswerBook package:

The installation software requires you to designate a parent directory for each AnswerBook package, as they are installed one by one.

Typically, AnswerBook packages are installed in */opt*, but they can be installed in any appropriate directory under *root* (*/*) with enough disk space.

In a separate command window:

1. Check available disk space in the directories under the *root* partition.

df -k

2. Compare the available space in the list with the sizes listed for the nil and heavy installations.

In the example below, the system has enough space in the */opt* partition to do a heavy installation of an AnswerBook package under 18 Mbytes.

df -k

Filesystem	kbytes	used	avail	capacity
Mounted on				
/dev/dsk/c0t0d0s5	31966	10837	17939	38%
				/opt

e. Finish the installation:

Choose an installation option to proceed:
Enter the number of an installation option from the list
above (1 or 2).

1. Type **1** for nil, **2** for heavy.

2. Type the name of the parent directory for the package.
The default is
/opt:

Specify the parent of the AnswerBook home directory:

/opt (recommneded)

3. Type **y** to complete the installation.

Do you want to continue with the installation of this
package? [Y, n, ?] **y**

The installation proceeds, listing AnswerBook components as
they are installed, until you see this message:

Installation was successful.

[information varies...]

Select package(s) you wish to process (or 'all' to
process all packages). (default: all) [?,?,q]: **q**

4. Type **q** to quit the installation.

5. View the list of installed packages:

pkginfo | grep AnswerBook

You'll see a list of all installed AnswerBook packages.

6. Check the installation accuracy of each installed package:

pkgchk packagename packagename packagename [and so on]

NOTE: The *pkgchk* process takes time, even for one package.

f. Start AnswerBook by command.

In an xterm window, type the following:

```
# setenv OPENWINHOME /usr/openwin  
# /usr/openwin/bin/answerbook
```

NOTE: In setting the environment variable OPENWINHOME , you must give the exact path /usr/openwin. You must have OpenWindows installed locally in /usr/openwin or mounted on /usr/openwin.

g. Removing an AnswerBook Package

You may decide to change the installation type for your AnswerBook package. For example, you may have chosen the nil option, but now want to install the complete heavy AnswerBook package.

First remove the AnswerBook package.

1. As *superuser*, type:

```
# pkgrm {packagename}
```

CAUTION: Do not remove AnswerBook packages or AnswerBook-associated files using the *rm* command. Using the *rm* command will corrupt the record keeping of AnswerBooks on the system. Using *pkgrm* is the only valid way to remove AnswerBook packages.

2. Verify you want to remove the package:

The following package is currently installed.

{Packagename}

Do you want to remove this package? y/n/q? **y**

SECTION 20. DISK DUPLICATION PROCEDURES

To speed creation of SPARC-5 application clients, a disk-to-disk copy procedure can be used. Although this procedure is used at some sites, it is not recommended for general use because of per-application efforts required to change host names.

This procedure is a manual disk duplication procedure for use with GCCS workstations. It assumes that the SOURCEDISK is a 2.1-GB external hard disk connected via a SUN SCSI cable to a SPARC-5 workstations and the TARGETDISK is a 2.1-GB external hard disk connected to the SOURCEDISK via a SCSI cable. If 1.05-GB external hard drives are used, the procedure will work; however, both the SOURCEDISK and TARGETDISK should be the same size. This procedure also assumes that the network information system used is NIS+. For e-mail in GCCS, DNS must be updated, but that issue is not addressed by this procedure.

20.1 Lessons Learned:

- A disk configured for a SPARC-5 will not work on a SPARC-20 and vice versa.
- If the command *boot -rs* is not used during the boot-up prior to duplication, Solaris may not recognize the second SCSI device (TARGETDISK). If Solaris does not recognize the existence of the TARGETDISK, the SOURCEDISK will attempt to duplicate itself to a file on the source drive (see below, Step 1).

20.2 Initial Conditions:

- The workstation is off.
- A SOURCEDISK containing the desired GCCS workstation configuration is ready to be duplicated to the TARGETDISK(s) to be fielded.
- The SOURCEDISK workstation's boot device should be *disk*.

20.3 Procedure:

- a. On the back of the TARGETDISK, set the SCSI address to **5** by pressing the buttons above or below the address indicator.
- b. On the back of the SOURCEDISK, verify that the address of the SOURCEDISK is 3.
- c. Connect the workstation, SOURCEDISK, and TARGETDISK with SCSI cables. Ensure that the SCSI bus is properly terminated.
- d. Turn on the SOURCEDISK and the TARGETDISK.

- e. Turn on the workstation. Take the workstation to the ok prompt by pressing **<STOP> A** during the memory initialization process of the boot up.
- f. At the ok prompt, type:

boot -rs <enter>

This boots the workstation to single-user mode and reconfigures the workstation and dev directory so that it recognizes the TARGETDISK.

- g. When prompted, enter the root password to enter maintenance mode.
- h. At the # prompt, type:

format <enter>

The only purpose of using *format* is to verify that the SOURCEDISK and the TARGETDISK are recognized by the operating system. *format* will display the drives currently recognized by the system. There should be two 2.1-GB drives, one at c0t3d0 (SOURCEDISK) and the other at c0t5d0 (TARGETDISK).

- i. When prompted *Specify disk (enter its number)*, type:

0 <enter>

This enables you to enter *quit* to leave the format function.

- j. At the <format > prompt, type:

quit <enter>

- k. At the # prompt type:

fsck <enter>

This will check the file system on the SOURCEDISK. If no errors are returned, proceed. If errors are returned, correct them and retest the functionality of the workstation prior to attempting disk duplication.

- l. At the # prompt, type:

**dd if=/dev/rdisk/c0t3d0s2 of=/dev/rdisk/c0t5d0s2 bs=64k
<enter>**

This command duplicates the SOURCEDISK (/dev/rdisk/c0t3d0s2) onto the TARGETDISK (/dev/rdisk/c0t5d0s2). The process takes 20-30 minutes for a 2.1-GB hard drive. If the TARGETDISK was not recognized by the *boot* -

rs command, then the dd command will attempt to place a duplicate of itself in a directory on the SOURCEDISK under the directory: /dev/rdisk/c0t5d0s2. It will also result in a short write (10 minutes) and return a "file system full" error. The file must be removed prior to attempting another duplication.

- m. If the duplication is successful, the # prompt will be returned.

- n. At the # prompt, type:

fsck /dev/rdisk/c0t5d0s2 <enter>

This will check the TARGETDISK. If no errors are found, proceed. Otherwise, attempt to locate/correct the error and either repeat the disk duplication or proceed.

- o. At the # prompt, type:

init 0 <enter>

This shuts down the workstation.

- p. At the ok prompt, turn off the SOURCEDISK and the TARGETDISK. Remove the SOURCEDISK from the SCSI bus. Attach the TARGETDISK to the workstation via a SCsicable. Ensure the SCSI bus of the TARGETDISK is properly terminated. Change the SCSI address on the TARGETDISK to **3**. Turn on the TARGETDISK. Ensure that the workstation is connected to the GCCS network.

NOTE: DO NOT ATTEMPT TO USE THE SOURCEDISK ON THE NETWORK UNTIL THE TARGETDISK DUPLICATION PROCESS IS COMPLETED!!!!!!!!!!!!!!

- q. At the ok prompt, type:

boot <enter>

This will boot the machine to the GCCS globe. Monitor the boot up to ensure that the boot up is proper.

- r. At the GCCS globe, log in as **root**.
- s. Select an xterm with the mouse cursor.
- t. Type:

cd /etc <enter>

This changes to the etc directory.

- u. Edit the *hosts* file. Remove the SOURCEDISK host name and IP address. Insert the TARGETDISK's new host name and IP address. Save the *hosts* file (see example below).

Example: (comments are in {})

```
# vi hosts <enter> {command to edit hosts}
```

{Below is the /etc/hosts before edit}

```
127.0.0.1 localhost loghost
128.84.170.134 gsw134 {SOURCEDISK hostname and IP address}
128.84.190.1 dbserver emserver gdb1 mailhost {server info}
128.84.190.22 gap1 appserver1 {server info}
128.84.190.23 amhserver amhs {server info}
```

{After edit}

```
127.0.0.1 localhost loghost
128.84.170.135 gsw135 {TARGETDISK hostname and IP address}
128.84.190.1 dbserver emserver gdb1 mailhost {server info}
128.84.190.22 gap1 appserver1 {server info}
128.84.190.23 amhserver amhs {server info}
```

```
:wq! <enter> {quits the editor and saves the file}
```

- v. Edit the *nodename* file and replace the SOURCEDISK host name with the TARGETDISK hostname.
- w. Edit the *hostname.le0* file and replace the SOURCEDISK host name with the TARGETDISK hostname.

NOTE: If the TARGETDISK workstation is going to be placed behind a router different from the SOURCEDISK's router, the */etc/defaultrouter* file must also be edited so that the correct defaultrouter IP address is inserted.

- x. The next steps remove SOURCEDISK's nisplus information from the TARGETDISK.

- 1. Type:

```
rm /etc/.rootkey <enter>
```

This removes *.rootkey* file from */etc*.

- 2. Type:

```
rm -r /var/nis/* <enter>
```

This removes *NIS_COLD_START* and *NIS_SHARED_DIRCACHE* files.

y. Type:

init 0 <enter>

This shuts down the workstation. If applicable, disconnect the TARGETDISK from the duplication workstation and connect it to a workstation on the correct subnet. Ensure that the TARGETDISK workstation host name and IP address are in the current */h/EM/nis_files/hosts* file and that a *nispopulate* has been run since the update to the hosts file.

z. When ready to initialize the workstation, boot up the machine:

At the ok prompt, type:

boot <enter>

or, if the workstation is powered down, turn on the TARGETDISK and workstation and allow it to boot up.

aa. During the boot-up, monitor to ensure that the host name is the host name of the TARGETDISK, and no errors occur. If errors occur, troubleshoot them in single-user mode. While in single-user mode, *ping*, *snoop*, and other network functions can be accessed by performing the following steps:

```
cd /etc/rc2.d <enter>
./S69inet <enter>
./S72inetsvc <enter>
```

Other functions can be accessed by running other executables. See the Solaris Administrator's Guide for further information.

bb. After a proper boot-up, the machine should display the GCCS globe. Log in as **root**.

NOTE: IT IS ABSOLUTELY IMPERATIVE THAT A NISCLIENT INITIALIZATION BE PERFORMED IN MULTI USER MODE!!!!!!!!!!!!!!

cc. Select an xterm with the mouse cursor.

dd. Type:

```
/usr/lib/nis/nisclient -i -h {hostname of em server in  
/etc/hosts file} -d {nis domainname} <enter>
```

When prompted, type:

y <enter>

to continue the initialization.

NOTE: If this is the first time that a *nisclient -i* has been run on the TARGETDISK host name, then the secure nisplus password will be asked for. If it is a second or third initialization, only the root login password is required.

When prompted, enter the secure nisplus password.

NOTE: The secure nisplus password can be found when a *nispopulate* is run on the hosts file in the */h/EM/nis_files* directory (*nispopulate* must be run after updating the */h/EM/nis_files/hosts* file from the */h/EM/nis_files/update* directory).

When prompted, enter the root password.

If no errors occurred, this message will be displayed:

Client initialization complete!! Reboot machine for changes to take effect.

If an error occurs, the reason will be displayed. Correct the error then perform Steps x1 and x2 prior to attempting another *nisclient* initialization.

ee. If no errors occur, type:

init 6 <enter>

The workstation should reboot. Monitor the boot-up. If normal, the site should be able to log in using a valid user account. Test the workstation for proper functionality.

APPENDIX A. ORACLE RDBMS OVERVIEW

The GCCS Database is based on the ORACLE Relational Database Management System (RDBMS). This section provides a general overview of the ORACLE RDBMS. For specific information and operational instructions for ORACLE user access, backup/recovery procedures, ORACLE Database Administrator (DBA) utilities, SQL*Forms, SQL*Plus, SQL*Reports, and SQL*ReportWriter access, refer to the current version of the *ORACLE RDBMS Database Administrator's Guide* and the documentation for the particular products. The *Database Administrator's Guide* describes the GCCS database and GCCS database architecture, and presents detailed instructions for database administration activities. For GCCS, the ORACLE RDBMS is installed on the database server, either a SUN SPARCcenter 1000 or SPARCcenter 2000.

Logging onto a database server as *orabda* automatically starts the ORACLE Server Manager, a tool to browse and alter the database. In addition, an X window is available; it is iconized in the lower left corner of the screen.

To use the Server Manager, enter "/" for the user name and select **connect**. ORACLE system information is selectable by single-clicking on the desired option, e.g., STORAGE, SECURITY, INSTANCE, RECOVERY and SCHEMA. Much of what is done using the SQL*DBA commands is discussed below. ORACLE commands can be run by selecting **New Worksheet** from the **File** menu.

A.1 Understanding the ORACLE Database

This section provides an overview of the ORACLE Relational Database. This information is provided as an introduction for readers unfamiliar with database concepts. The current revision of the ORACLE vendor documentation is the comprehensive reference for using and administering the GCCS database.

An ORACLE database is a collection of data that is treated as a unit. The principal purpose of a database is to store or retrieve related information. An ORACLE database can be configured to lock out various features and portions of the database to ensure system security. The ORACLE database is accessed via an ORACLE instance (the software that manipulates the database) when the database is opened. When the database is closed, its data is unavailable to users.

The ORACLE RDBMS enables GCCS users to maintain, monitor, and manipulate large quantities of data in a structured environment. The ORACLE RDBMS offers GCCS users many benefits:

- Easy access to all data
- High transaction-processing performance

- High, controlled availability
- Flexibility in data modeling
- Manageable security, user hierarchy, and database-enforced integrity
- Reduced data storage and redundancy
- Independence of physical and logical data design
- A high-level data manipulation language (SQL)
- Portability, compatibility, and connectivity.

A.1.1 Database Structure. An ORACLE database has both a physical structure and a logical structure. The physical storage structure (Figure A-1) can be managed without affecting access to the logical storage structure.

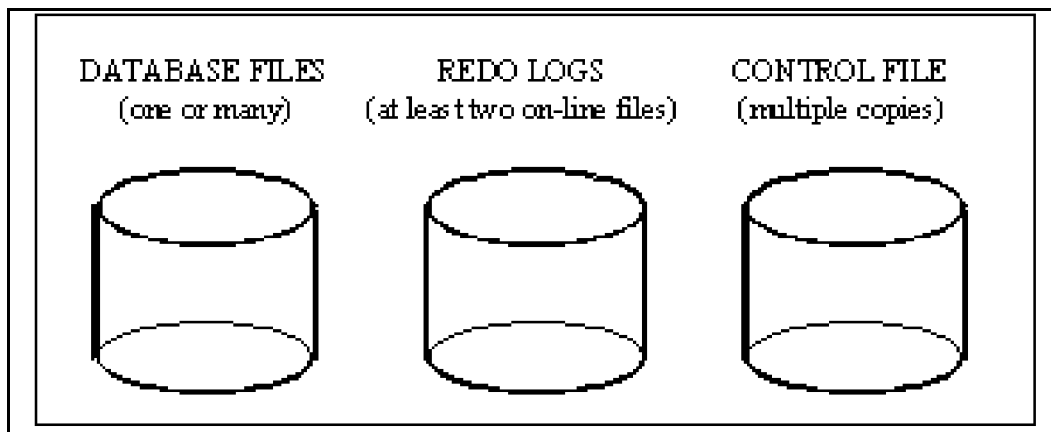


Figure A-1. The ORACLE Physical Database Structure

A.1.1.1 Physical Database Structure. An ORACLE database's physical structure is determined by the operating system files that constitute the database. Each ORACLE database consists of one or more data files, two or more redo log files, and several copies of the control file.

DATA FILES contain all the database data. They can be added or removed from a database, as required, to meet the user's needs. A data file can only be associated with one database, and its size cannot be changed once it is created.

REDO LOG FILES are a set of files that sequentially record all changes--whether committed or uncommitted--and are used to recover data not written to the database for some reason, such as system or media failure. The process of applying the redo log is called "rolling forward" or, more generally, "recovery."

CONTROL FILES record the physical structure of the database. A control file contains the database name, names, and locations of its data files, and the timestamp of database creation. Once an ORACLE instance is started, its control file is used to identify the

database and redo log files that must be opened and accessed for database operation. Control files are automatically updated by ORACLE and cannot be manually modified. One or more copies of the control file must be maintained for database backup.

A.1.1.2 Logical Database Structure. An ORACLE database's logical structure is determined by one or more storage units, called tablespaces, and the database's schema objects (such as tables, views, synonyms, indexes, sequences, clusters, and stored procedures).

TABLESPACES are used to group all of an application's objects to simplify certain administrative operations. A tablespace can be set *on-line* (accessible) or *off-line* (not accessible). The GCCS database has many tablespaces. The original tablespace name SYSTEM is created during ORACLE installation. The SYSTEM tablespace cannot be set off-line or removed.

All data in a tablespace is stored in segments. A SEGMENT is set of extents allocated for a logical structure. An EXTENT is a specific number of contiguous data blocks, obtained in a single allocation, used to store a specific type of information. A DATA BLOCK corresponds to a specific number of bytes of physical database space on disk. The DATA BLOCK size is unchangeable after database creation.

Most segments begin at some specified size (number of extents), and grow dynamically (adding extents), as required. The DBA can monitor the space usage (extents) of a tablespace by looking at these views in SQL*Plus using these commands:

```
select * from sys.dba_segments;
select * from sys.dba_extents;
select * from sys.dba_free_space;
```

NOTE: To display the structure of each view above, enter "DESC table_name" (e.g., DESC sys.dba_extents).

SCHEMA OBJECTS are logical structures that refer directly to the database's data. Schema objects include tables, views, synonyms, sequences, indexes, cluster, program units, and database links.

A TABLE is the basic unit of data storage in an ORACLE database. Table data is stored in rows and columns. Each table is defined with a table name and a set of columns. Each column is defined with a column name, a data type (Character, Varchar2, Number, and Date), and a width. A VIEW is a database object that is treated like a table. However, views do not actually contain or store data. Whenever the view is queried, it derives data from the base tables on which the view was defined. Hence, a view can also be considered

a *stored query*.

A SYNONYM is an alias for a table, view, sequence, or program unit. It is used to provide public access to an object, or to provide location transparency for tables, views, or program units on a remote database. A synonym can be either *public* (available to all users) or *private* (available only to a single user).

A SEQUENCE is used to generate a serial list of unique numbers for numeric columns of a database table.

INDEXES are optional structures associated with tables and clusters. Indexes are created to increase the performance of data retrieval and enable the search of records in sorted order or the random access of particular records based on a user-specified key. This minimizes the number of accesses by the program and can increase the efficiency of the database. An index can be created on one or more columns of a table. Indexes are logically and physically independent of the data in the associated table. They can be dropped or created at any time with no affect on the tables or other indexes. Indexes can be unique or non-unique. Unique indexes guarantee that no two rows in a table have duplicate values in the columns that define the index, while non-unique indexes do not impose this restriction on column values.

A CLUSTER is a group of tables that share the same data blocks because they share common columns and are often used together. They are used to improve disk access time and data retrieval.

A PROGRAM UNIT refers to stored procedures, functions, and packages. A stored PROCEDURE or FUNCTION is a set of Structured Query Language (SQL) and Procedural SQL (PL/SQL) statements grouped together as an executable unit to perform a specific task. A PACKAGE is used to encapsulate and store related procedures, functions, and other packages constructed together as an executable unit in the database. A DATABASE TRIGGER is a stored procedure that is implicitly executed (fired) when an INSERT, UPDATE, or DELETE statement is issued against the associated table.

A KEYWORD is a named object that describes a path from one database to another. It is implicitly used to access data on the remote database.

A.1.2 Database User Access and Privileges. Privileges provide control and management of access to a database. Before privileges can be granted to a user, a UNIX account and an ORACLE account must have been created (Section 9 details these procedures). Privileges can be assigned in two different ways:

DIRECTLY TO USERS

Privileges can be granted to a user explicitly (directly).

For example, a privilege to delete a record from table X_TEST in the database can be granted explicitly (directly) to the user SMITH.

ROLES

A role is a collection of data access privileges, system privileges, and/or roles, which can be granted to and revoked from users. Privileges can be granted to *roles*, and each role can be granted to one or more users. For example, a privilege to insert a record in the COUNTRY_CODES can be granted to the role GCCS_USER, which in turn can be granted to the users SMITH and JOHN. A privilege to execute a particular application can be granted one or more roles, and these roles can then be granted to the appropriate users. Roles facilitate the maintenance of privileges. Figure A-2 shows a sample role/privilege setup.

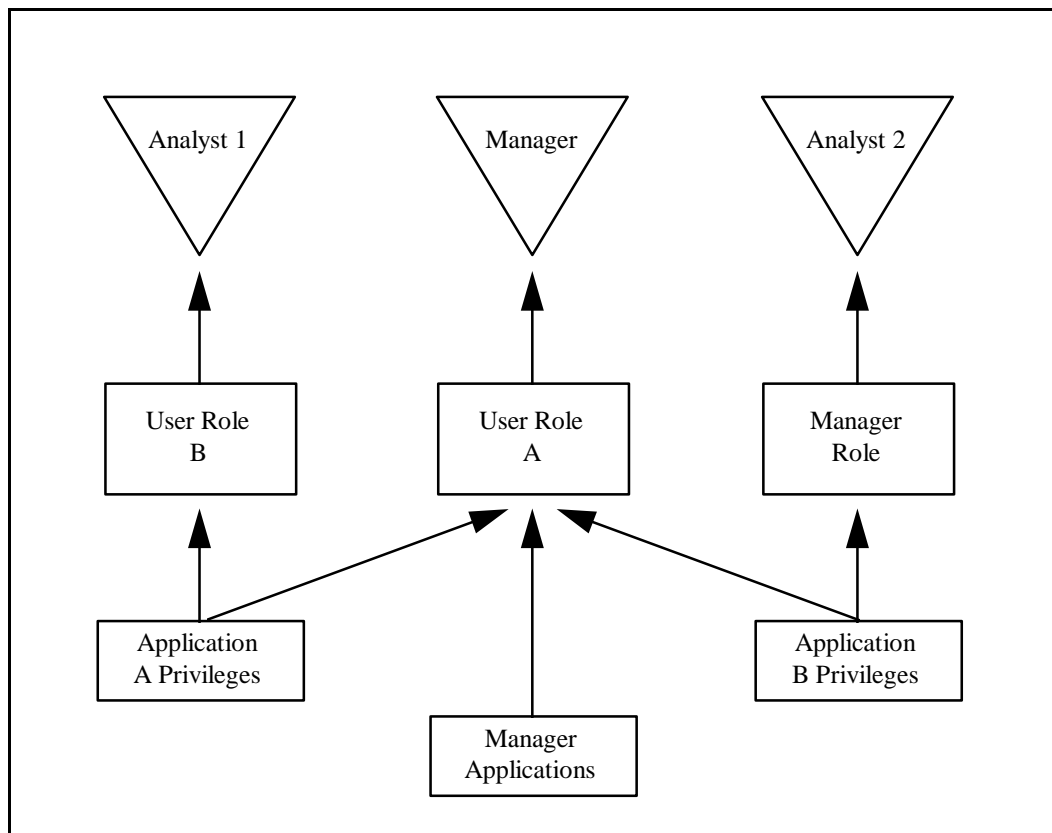


Figure A-2. Role/Privilege Setup

Roles can be provided by the DBA for individuals and groups of users for easy and controlled privilege management such as reducing privileges, dynamic privilege management, selective availability of

privileges (enable or disable), application awareness, and application-specific security. A role can also be granted to other roles, which in turn can be granted to one or more users. Roles can be enabled or disabled at the user level.

The highest level of privileges and access to a database must be limited to the DBA(s). To access a database, ordinary users must have a valid ORACLE user name and password, must have the "connect" role (a collection of privileges), and may or may not have the resource and/or DBA roles that are granted by the DBA.

The CONNECT role allows a user to connect to a database and view information in the ORACLE data dictionary. A user who possesses only the connect role cannot create, alter, or drop tables, indexes, views, synonyms, clusters, or sequences.

The RESOURCE role allows a user to create, alter, and drop tables, indexes, views, synonyms, clusters, and sequences. With the resource role, a user can grant or revoke schema objects to and from other users. A user with the resource role must also have the connect role.

The DBA role allows users to:

- Access any user's data and perform any SQL statement upon it.
- Grant and revoke database system privileges.
- Create public synonyms, public database links, roles, and user accounts.
- Control system-wide auditing and table-level auditing defaults.
- Perform database exports and imports.
- Perform database-wide maintenance operations such as adding tablespaces, data files, setting tablespace on- or off-line, backing up tablespaces, and archiving log files.

The IMP_FULL_DATABASE role allows users to select any table, back up any table, and insert, delete, and update certain system tables.

The EXP_FULL_DATABASE role allows users to log on as other users when performing full database imports.

A.1.3 ORACLE Database Startup and Shutdown. An ORACLE database is not always available to all users. To have control over the current status of an ORACLE database, only the DBA can start up or shut down the ORACLE database. When a database is open, users can access the information in it. When a database is closed, users cannot access the information. This is desirable, at times, to prevent users from corrupting the database while diagnostic and maintenance procedures are being carried out.

For specific instructions, refer to Sections A.1.5.1 (Database Startup) and A.1.5.2 (Database Shutdown).

A.1.4 Database Recovery and Backup. Database recovery and backup enables the restoration of damaged data and/or control files. If hardware, software, network, process, or system failure occurs, the database must be recovered as quickly as possible so normal operations can be resumed. Several problems can halt the normal operation of an ORACLE database or affect writing database information to the disk. The most common types of failure are:

USER ERROR FAILURE is caused by users, such as when someone accidentally drops a table.

STATEMENT FAILURE occurs when there is a logic failure in the handling of a statement in an application program. An error code or message is returned.

PROCESS FAILURE is the failure of the user, server, or background process in a database instance (e.g., an abnormal disconnect or process termination).

INSTANCE FAILURE occurs when a problem arises that prevents a database instance from continuing to work. This failure can result from either a hardware problem (such as a power outage) or a software problem (such as an operating system crash). An instance recovery is automatically performed as part of the next instance startup.

NETWORK FAILURE occurs when communication networks (such as the local area network, phone lines, etc.) are aborted (disconnected) on a distributed database system. This failure can interrupt the normal operations of a database system.

MEDIA FAILURE is a physical, non-recoverable error which can arise when trying to read or write a file that is required to operate a database. For example, a disk head crash causes the loss of all files on a disk drive.

A.1.4.1 Database Recovery. Several different features give the DBA flexibility when recovering databases:

ROLLING FORWARD reapplies all changes recorded in the redo log to the data files.

ROLLING BACK reverses the uncommitted database transactions recorded in the rollback segments and returns the database to a known stable point while the database is running.

ARCHIVING saves data found in the on-line redo logs for possible later use while the database is running. This feature protects the

database from disk failure, providing for complete recovery right up to the moment before failure.

An IMAGE BACKUP performs block-by-block copying while the database is shut down. Image backups can be done on individual tablespaces as well. If required, this type of physical backup can recover the status of the entire database.

The EXPORT utility enables a logical backup of selective data or an entire database to a file while the database is running. The exported files can be saved on disk or archived to tape.

The IMPORT utility enables restoration of logical data to the database from an exported file while the database is running.

A.1.4.2 Database Backup. Database backups safeguard against potential media failures that can damage files. Routine, periodic backups provide the best protection against data loss and corruptions. Database backups can be performed whether a data file is on- or off-line.

A.1.4.2.1 Off-Line Database Backups. Any data file can be backed up when the database is shut down or a tablespace is off-line. Database backup and recovery are available via a menu-driven interface under the RECOVERY directory. Refer to the *GCCS/JOPES System Services Administrators Manual*. The general procedures for off-line backups are:

- a. Shut down the database using either shutdown immediate or shutdown abort procedures as described in Section A.1.5.2 (Database Shutdown).
- b. Compress all ORACLE database files. Application database files are not stored under \$ORACLE_HOME:

compress APPLICATION_1/*.dbf
compress APPLICATION_2/*.dbf
- c. Copy all data files, on-line redo log files, and control files to tape by following these procedures:
 1. tar the ORACLE database files to tape using the applicable command for your site. The following commands assume a DAT tape is being used:

(1) (For an HP)

```
tar cvf /dev/rmt/3m APPLICATION_1/*.dbf.Z
tar cvf /dev/rmt/3m APPLICATION_2/*.dbf.Z
OR
cpio -ocBuv APPLICATION_1/*.dbf.Z>/dev/rmt/3m
```

```
cpio -ocBuv APPLICATION_2/*.dbf.Z>/dev/rmt/3m
```

(2) (For Sun)

```
tar cvf /dev/rmt/0bmn $APPLICATION_1/*.dbf.Z
tar cvf /dev/rmt/0bmn $APPLICATION_2/*.dbf.Z
OR
cpio -ocBuv $APPLICATION_1/*.dbf.Z>/dev/rst0
cpio -ocBuv $APPLICATION_2/*.dbf.Z>/dev/rst0
```

2. tar the `$ORACLE_HOME/dbs` directory to tape using the applicable command. The following commands assume a DAT tape is being used:

(For Sun)

```
tar cvf /dev/rmt/0bmn $ORACLE_HOME/dbs
```

3. tar the `/h/data/global` directory to tape using the applicable command. The following commands assume a DAT tape is being used:

(a) (For an HP)

```
tar cvf /dev/rmt/3m /h/data/global
```

(b) (For Sun) (8mm tape)

```
tar cvf /dev/rmt/0bmn /h/data/global
```

4. To preserve any messages that have been created, tar the `/h/USMTF/data` directory to tape (do this for each machine):

(a) (For an HP)

```
tar cvf /dev/rmt/3m /h/USMTF/data
```

(b) (For Sun)

```
tar cvf /dev/rmn/0bmn /h/USMTF/data
```

NOTE: See the Sun Solaris or HP Reference Manual for more details about the UNIX **tar** and **cpio** commands.

5. Repeat Steps 1, 2, 3, and 4 to ensure that there is a backup for each tape.

d. Restart the database:

1. Uncompress the ORACLE database files:

uncompress \$APPLICATION_1/*.dbf.Z
uncompress \$APPLICATION_2/*.dbf.Z
2. Start up the ORACLE database.
3. Start up the AUDIT TRAIL, QUEUE MANAGER, and tti.
4. Start traffic from MDT to GCCS (if AMHS is installed on the platform).
5. Start all other GCCS processes.

A.1.4.2.2 On-Line Database Backups. An on-line backup can be performed while the database is running. Thus, the DBA need not shut down the database to archive data. Data that is being accessed can also be archived during an on-line backup.

ORACLE can be operated in two archiving modes: *archived* and *noarchived*:

ARCHIVED MODE

When a database is operating in the *archived* mode, the on-line redo logs are saved before they are overwritten and the most recent backup can be used as part of data recovery. After restoring the necessary data files from the backup, database recovery can continue by applying archived and current on-line redo log files to bring the restored data files current. The files assembled by a full backup can be used to restore damaged files as part of database recovery from disk failure.

NOARCHIVED MODE

When a database is operating in the *noarchived* mode, the redo log files are overwritten without being archived and the most recent backup can be used to *restore* (not *recover* the database). Because the archived redo log files are not available to bring the database current, all database work performed since the database backup must be repeated. A full backup is the only method available to partially protect the database against disk failure.

The ON-LINE REDO LOG consists of at least two files that store all changes made to the database as they occur: one is optionally being spooled while the other is being written. These files are re-used once they fill up and are written to disk. At a minimum, archived redo logs that date back to the beginning of the oldest usable off-line database backup must be saved. The latest on-line redo log must also be saved. Archived redo logs previous to the last full backup can either be moved to tape or deleted.

A.1.5 Accessing ORACLE DBA Utilities. The ORACLE SQL*DBA is a DBA-management utility that performs these tasks:

- ORACLE instance starting and stopping
- ORACLE database mount, dismount, open, and close
- Monitoring of ORACLE database real-time use and performance
- Backup and recovery of database logs and data
- SQL statement execution
- PL/SQL statement execution.

Functions are selected from menus or initiated with commands from the operating system prompt. The SQL/DBA utility can be invoked from either *line* mode or *menu* mode (the menu mode is not discussed here). See Sections A.1.5.1 (Database Startup) and A.1.5.2 (Database Shutdown) for specific examples of how to use ORACLE DBA Utilities. To invoke SQL/DBA in *line* mode:

a. Enter:

sqlldb lmode=y

or

mode=line

<Return>. The SQL/DBA> prompt is then displayed.

b. For PL/SQL statement execution, enter:

connect <username> / <password>

<Return>, and the statement or series of statements to be executed.

For all other DBA functions, enter "connect internal" <Return>, and the command(s) necessary to perform the intended operation(s). Refer to the current revision of the *ORACLE Utilities User's Guide* for further information.

NOTE: SQL commands can be entered in either upper- or lower-case.

c. To exit SQL*DBA, enter:

Exit

NOTE: During a shutdown or startup of the database server, ORACLE shutdown and startup is handled by scripts invoked by the operating system.

A.1.5.1 Database Startup. Follow these steps to start up a database:

- a. Log onto the database server if necessary.
- b. Invoke SQL*DBA:

1. Enter:

sqldba lmode=y

or

mode=line <Return>.

2. At the SQLDBA> prompt, enter:

connect internal <Return>.

3. Enter:

startup <Return>.

(ORACLE will automatically start an instance, mount, and open the database.) Observe the display of messages acknowledging the startup of the database.

4. To quit SQLDBA when done: enter

Exit.

A.1.5.2 Database Shutdown. An ORACLE database can be shut down using one of three options:

SHUTDOWN NORMAL

ORACLE waits for currently enrolled users to disconnect from the database, prohibits new users from logging, closes and dismounts the database, and shuts down the instance. Shutdown normal is accomplished via the "shutdown" or "shutdown normal" command.

SHUTDOWN IMMEDIATE

ORACLE immediately terminates any current client SQL statement being processed (does not wait for users currently connected to the database to disconnect) and rolls back the uncommitted statements. (This option should be used when a reboot or power shutdown is anticipated, or when the database is functioning irregularly.) Shutdown immediate is accomplished by entering "shutdown immediate" instead of "shutdown." This was an early shutdown option for GCCS.

SHUTDOWN ABORT

Following shutdown abort option, the database instance is aborted immediately, uncommitted transactions are not rolled back, and the next startup of the database will require instance recovery procedures (automatically performed during database startup). (In earlier versions of ORACLE this option was used only when both normal and immediate shutdown failed, or when having difficulty starting a database.) Under normal GCCS circumstances, the shutdown abort option is the default condition. It is not as violent as the name implies, and it ensures the database shuts down.. Shutdown abort is accomplished by entering "shutdown abort" instead of "shutdown."

These steps are required to shut down an open database:

- ```
a. Enter:

 sqldba lmode=y <Return>.

b. Enter

 connect internal <Return>.

c. Enter

 shutdown normal

or

 shutdown immediate

or

 shutdown abort <Return>.
```

```
(ORACLE will automatically close and dismount the database and shut
down the instance.)
```

Observe the display of messages acknowledging the startup of the database.

- d. To quit sqldba when done, enter:
- Exit.**

**A.1.1.6 Accessing SQL\*PLUS.** SQL\*Plus is an ORACLE tool that enables users to use Structured Query Language (SQL) or Procedural Language/Structured Query Language (PL/SQL) to query, update, delete, create, and modify database tables. In GCCS, SQL\*Plus is usually

invoked via corresponding UNIX account (sometimes referred as the OPS\$ account), as shown:

```
sqlplus /
```

To invoke SQL\*Plus with an internal ORACLE account, enter:

```
sqlplus
```

at the operating system prompt,

```
{username}
```

at the username prompt (where {username} is a valid ORACLE account name), and

```
{password}
```

at the password prompt (where {password} is the password associated with the user name provided).

The sql> prompt is displayed, enabling the entry of SQL commands. Refer to the current revision of the *ORACLE SQL Language Reference Manual* or *SQL\*PLUS User's Guide* for more information on SQL commands.

---

**NOTE:** User access to SQL\*PLUS is a data security problem. JOPES users should not have access to SQL\*PLUS or any COTS database browser, because they have JOPES Core Database access, and the use of SQL\*PLUS would allow them to bypass the security measures incorporated in the JOPES applications.

---

---

**NOTE:** SQL commands can be entered in either upper- or lower-case.

---

**A.1.7 Passwords.** Each ORACLE database user account requires both an ORACLE user name and password. User accounts are created by the DBA. As required, the DBA can change privileges for any user. For security and monitoring purposes, the ORACLE user account is tied to the UNIX account. Thus, a separate ORACLE password is not required and is not provided. Creating user accounts is described in Section 9.

In GCCS, user names are created as "identified externally." These are also referred to as OPS\$ accounts. This allows for automatic logins to the database during which ORACLE reads the UNIX operating system user account to authenticate each user's status. This process eases user logon into ORACLE. ORACLE users can be externally logged onto ORACLE-based applications. Thus, an application or tool can be invoked without having to manually enter <username> and <password> each time the database is accessed.

Example: to invoke *sqlplus* on an Xterm from within a specific user account, enter: "sqlplus /", then the sql> prompt appears.

**A.1.1.8 Maintaining SQL\*Net.** SQL\*Net is ORACLE's remote data access software and enables client/server communications across the network. GCCS is currently running both SQL\*Net Version 1 and SQL\*Net Version 2. Version 1 is available only for any backwards-compatibility situations and long-term support is not guaranteed.

For an application on a client machine to communicate with the ORACLE database, there must exist a listener to field the requests and forward them to the specified database. There are currently two listeners running in GCCS, one for the SQL\*Net V1 interfaces, *orasrv*, and one for the SQL\*Net V2 interfaces, *tnslsnr*. The listeners run only on the database server. The network protocol is TCP/IP; GCCS exists on this single protocol community.

In order to run the several SQL\*Net tools described below:

```
su - oradba
```

**A.1.1.9 SQL\*Net V1.** To determine whether SQL\*net V1 is running on the database server:

```
tcpctl stat
```

alternately:

```
ps - ef | grep orasrv
```

where *orasrv* is the name of the V1 listener on the database server to start the V1 server:

```
tcpctl start
```

To stop the V1 server:

```
tcpctl stop
```

The connection string of the V1 connection could, for example, be set:

```
T:dbserver:GCCS
```

**A.1.1.10 SQL\*Net V2 .** The default ORACLE network connection for GCCS is SQL\*Net V2.1. Sourcing the ORACLE environment, therefore results in (among other things)

```
TWO_TASK = gccs.world
```

where *gccs.world* is a connection string that identifies the local ORACLE database server. This is described in greater detail below. To determine whether SQL\*Net V2 is running on the database server:

**lsnrctl stat**

Alternately:

**ps -ef | grep tnslnr**

where *tnslnr* is the name of the V2 listener on the database server machine. If it becomes necessary to start the V2 listener:

**lsnrctl start**

To stop the V2 server:

**lsnrctl stop**

There are three ascii files associated with the V2 software. On the GCCS database server they are stored in the */var/opt/oracle* directory. These are:

**listener.ora  
tnsnames.ora  
sqlnet.ora**

For the client machines, only *tnsnames.ora* and *sqlnet.ora* exist under */var/opt/oracle*. If it becomes necessary to edit these files, a UNIX editor such as *vi* can be used. One must be careful not to inadvertently add or delete any "extra characters" in these files, in particular, trailing parentheses. These files can also be maintained via the GUI tool *Netman*, which is discussed below.

Examples of valid V2 connection strings are:

**gccs.world  
acc\_db.world  
nmcc\_db.nmcc.gcc.smil**

The default GCCS connection string, that value to which *TWO\_TASK* is set, is *gccs.world*, which references the local database server machine. The file */var/opt/oracle/tnsnames.ora* defines the connection information. This file contains data for each of the principal JOPES Core Database servers in addition to the local database server. If the local server is a JOPES Core Database, then it may be identified twice in this file.

A connection string, also called a service name, maps to a connect description stored in the network configuration file *tnsnames.ora*. A connect description is a specially formatted description of the destination for a network connection, consisting of sets of keywords and values. It lists the communities of which the client is a member, the community protocol, e.g., TCP/IP, host name (or alternately, IP address) and the UNIX port number allocated. The *tnsnames.ora* file

resides on each client and database server machine. If connection data changes them, each copy of this file should be updated. This onerous task will be eventually (or soon) replaced by a centralized maintenance scheme.

**A.1.11 ORACLE Network Manager.** The network manager, *netman* is a GUI tool provided by ORACLE to facilitate maintenance of the SQL\*Net V2 data. Network management is divided into a number of components, which are depicted on the main window as:

- Domain
- Community (protocol)
- Node
- Protocol Interchange
- Database Listener
- ORACLE Database
- ORACLE Gateway
- Name Server
- Client Profile
- Local Region
- Service Names Alias
- SQL\*Net V1 Connect String.

The following steps briefly describe the procedure to follow to update the `/var/opt/oracle/*.ora` files using the network managers:

1. **setenv DISPLAY local\_machine:0.0**
2. **netman**

Two windows pop up, one behind the other. The front window lists the network components as listed above. From the back window select **File** and then **New** or **Open**. If **Open** is selected, the filter window pops up with two choices:

- File System**
- Database**

Select **File System** and **OK**.

The resulting pop-up window has a Filter area, Directories and Files scroll areas, and an OPEN FILE line. Enter either a fully-qualified File name or use the Filter key, Directories, and Files to override the current selection. File names end in "NET", e.g., GCCS\_DB.NET.

Press **OK**. In the main window, there are (at least) two entries in the right-hand scroll area, root and World. If Community is selected instead of Domain, TCP/IP shows up on the right. Any of the right-side entries can be selected and edited. Probably the most common change will be the HOST field under the Database Listener selection. After selecting a particular database listener, edit it. In the Addresses area that appears, double-click on TCP:1526, make the necessary changes in the "Host" line of the resulting window, and select **OK** to exit each window.

When all changes have been entered, select **Save** or **Save As** under the "File" menu, then select **Validate**. If all objects are valid, select **Generate to a File System**.

A directory for each Listener is generated, and each contains a *listener.ora*, *tnsnames.ora*, and *sqlnet.ora* file. Because GCCS sites are identical from a configuration standpoint, the files from any one of these directories can be disseminated onto the server and client machines.

To shut down the SQL\*Net V2 listener, before editing these files, on the database server machines as *oradba* enter:

```
lsnrctl stop
```

Save ("mv") the existing three files in */var/opt/oracle* and copy the new ones in their place.  
Restart the listener:

```
lsnrctl start
```

**A.1.12 Full System Export.** To export the entire database, for whatever reason, including backup or to populate another machine, the following file can be created as described below:

```
File exp_full.par:

userid = system
full = Y
compress = N
file = exp_full.dmp
log = exp_full.log
```

To run, go to the directory where the export will reside and enter:

```
exp parfile=exp_full.par
```

You will be queried for the ORACLE "system" password. *oradba* will need privileges to write into that directory. Allow 700 MB for the export file.

Alternatively, there may be export procedures provided by SMDB (the JOPES Core Database).

**A.1.13 Creating New User Tables.** Each GCCS user has his/her own account in the ORACLE database. Users can create tables using SQL\*Plus if they have access to it, usually via an xtern. The new tables are stored in the user's default tablespace. The *ORACLE SQL Language Reference Manual* and the *ORACLE SQL\*Plus User's Guide* provide more information on the available commands. This is not a normal GCCS activity.



**A.1.14 Correcting Database Fragmentation.** A message pileup occurs when the maximum number of extents for a table is exceeded. The following procedure provides a solution to this problem:

- a. As the owner of the data, export the relevant table using the ORACLE export command (enter **exp** and the export target, then respond to the program queries).
- b. When running the export command, answer *no* to the query "Compress extents?".
- c. Drop the relevant table using SQL\*Plus.
- d. Import the saved table by using the ORACLE import command (enter "imp" and the import target, then respond to the program queries) and answering *yes*. Ensure that the answer to "import grants?" is *yes*.

This procedure must be accomplished without any user or process accessing the relevant table.

## **A.2 Determining Free Space in a Tablespace.** TBS

### **A.3 Database Monitor Routines**

The ORACLE routines described in this appendix are used to monitor the state of the database. They can help to avoid problems and aid in troubleshooting errors, especially when problems occur while adding users. The reports generated by these routines indicate when the system tablespace is full. Adding another file to the system tablespace can often correct these problems.

These utilities are very useful when a tablespace becomes too full or when a database object attempts to exceed its MAX\_EXTENTS. The database can be monitored daily and status reports can be produced. This process enables the DBA to spot and eliminate many potential problems before they occur. Also, the routines enable the DBA to regulate and schedule some of the database "repair work."

These c shell routines can be run daily by placing them in the DBA's *crontab* file. When this is done, the routines will access the database at the designated time and will create an output file containing useful information about database storage space. The script file can concatenate the information files and e-mail them to interested parties. The programs were designed to be run weekly, but they can easily be run daily. It requires one month to accumulate a usable amount of data in the CHANGED column of the reports.

## **APPENDIX B. ENGINEERING EVALUATION OF PC X-SERVERS AND PC TCP/IP PRODUCTS**

### **B.1 Introduction**

Originally, Transmission Control Protocol/Internet Protocol (TCP/IP) was used only with UNIX workstations and mainframes; TCP/IP is now available to all popular desktop Operating Systems (OSs) and platforms. TCP/IP provides a simple, standardized means of connecting large, heterogeneous networks. Working with TCP/IP are PC X-Servers, which provide to PCs the ability to display X Windows-based applications found on UNIX workstations, thereby allowing users to keep their favorite PC applications while gaining the ability to run applications found on big UNIX workstations.

This appendix describes the evaluation of four PC X-Servers and two TCP/IP products that were nominated as GCCS Common Operating Environment (COE) applications.

### **B.2 Evaluation Criteria and Product Evaluated**

#### **B.2.1 PC X-Servers**

**B.2.1.1 Criteria.** PC X-Servers were evaluated based on the criteria listed below:

|                       |                                                                                                                                                                                                                                                          |
|-----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Networking:</b>    | Did the X-Server work with many networking products and was the interface with those products well documented?                                                                                                                                           |
| <b>Features:</b>      | Are the networking tools and desktops that the X-Server provides useful and valuable?                                                                                                                                                                    |
| <b>Installation:</b>  | Did the X-Server offer standard and custom installs? Were multiple installations needed to load other required networking packages? Did the X-Server find the existing network? Was it easy to configure the server? Will it be easy to start X clients? |
| <b>Performance:</b>   | Did the clients start quickly? Was interactive performance acceptable?                                                                                                                                                                                   |
| <b>Stability:</b>     | Did clients crash the server or suffer from X errors? Are enough winsockets available for multiple X windows?                                                                                                                                            |
| <b>Documentation:</b> | Was it complete and thorough? Did it provide specific information about supported network interfaces?                                                                                                                                                    |

**B.2.1.2 Products Evaluated.** The following PC X-Server products were evaluated:

- eXceed 4 for Windows by Hummingbird Communications Ltd.
- XoftWare/32 for Windows by AGE Logic, Inc.
- PC-Xware by Network Computing Devices, Inc.

- Reflection-X by Walker Richer and Quinn, Inc.

**B.2.2 TCP/IP Products.** The TCP/IP products were judged on six main categories: setup, performance, documentation, support, value, and winsockets. The category of performance was divided into three subcategories: RAM consumption, Network File System (NFS), and file transfer. The categories are listed below.

**B.2.2.1 Criteria.**

|                       |                                                                                                                                                                                 |
|-----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Setup:</b>         | How easy or difficult was each application to install and did the vendor provide an intuitive, interactive interface for the process?                                           |
| <b>Performance:</b>   | How much memory did the TCP/IP products consume? How fast was the TCP/IP stack as measured using the Socket Wrencher test tool?                                                 |
| <b>Documentation:</b> | Is the documentation accurate, did it provide useful diagrams and a comprehensive index?                                                                                        |
| <b>Support:</b>       | Is technical support available?                                                                                                                                                 |
| <b>Value:</b>         | The value of the product will be determined by its overall performance, ease of use, features, and bundled utilities provided.                                                  |
| <b>Winsockets:</b>    | How many winsockets are supported? What type of driver implementation is used? (Please refer to Appendix B for a detailed description of the different driver implementations.) |

**B.2.2.2 Products Evaluated.** The following TCP/IP products were evaluated:

- Microsoft VxD 32 TCP/IP.
- Chameleon/NFS TCP/IP.

**B.3 PC X-Server Products**

**B.3.1 Summary of Findings.** The product eXceed 4 for Windows is comprehensive, with a good set of features, easy installation, and good documentation. It also had the most problems running GCCS mission applications. It was impossible to move or iconize the UCCS session manager banner using eXceed 4 for Windows, and the TPFDD editor crashed in certain instances. Reflection-X worked well and installed easily but was confusing to use, thereby making it a more difficult package to integrate with GCCS. NCD's PC-Xware has simple organization, allows remote configuration, and currently has the best user interface. However, PC-Xware was also unable to move or iconize the session manager banner. If being unable to move or iconize the session manager banner is unimportant, PC-Xware may serve GCCS well. XoftWare/32 is a comprehensive package without obvious flaws. It is well organized and simpler to use than any of the other packages reviewed. It worked the best with GCCS applications during the evaluation period. It is also the least expensive.

### **B.3.2 Product Reviews**

#### **B.3.2.1 eXceed 4 for Windows**

##### **B.3.2.1.1 Product Overview**

**Vendor/Product:** Hummingbird Communications Ltd./eXceed 4 for Windows

**Phone:** 415-917-7300

**Fax:** 415-917-7310

**Address:** 480 San Antonio Rd., #100  
Mountain View, CA 94040

**B.3.2.1.2 Product Description.** Hummingbird's eXceed 4 for Windows is a PC-to-UNIX/X Windows integration software suite that allows PCs running Microsoft Windows to display and utilize X applications running on host computers, such as UNIX and VMS.

- **Main Server Features:**
  - 32-bit PC X-Server.
  - Windows based installation/configuration.
  - Network administration facilities.
  - X11R5 compliance.
  - Bundled VxD-based TCP/IP network software.
  - Serial access to X hosts over telephone lines, using eXceed/Xpress.
  - Single and multiple windowing modes.
  - Host based (Motif, OpenLook, etc.) or local window managers (either Windows or Hummingbird's own local Motif-like window manager may be used as the local window manager).
  - eXceed Basic scripting language (proprietary).
  - Launch Pad and Virtual Desktop facilities.
  - X Development Kit, to develop and run X Windows clients locally, on your PC.
- **Communications Features:**

Many start-up methods, including:

  - TELNET, REXEC, RSH, RLOGIN, dterm, PCX\$SERVER, XDMCP, hrps.
  - Support for local XDMCP Display Manager Chooser, presenting a list of hosts willing to manage the X display.
  - Application start-up options, such as X start point and click start-up of X and character-based non-X applications, and X session drag-and-drop, point and click start-up of multiple X, Windows, and non-X applications.
  - Includes an icon library for custom icon installation for X start, W start, and X session Transport Monitor provides visual feedback of transport activity.
  - Telnet support for VT320/220/100/52 emulation.
- **File Transfer and Management Features:**
  - FTP supports graphical drag-and-drop file transfer and directory management.
  - Local printing and eXceed Basic script driven file transfers.

- Supports Active FTP connections.
- Connection to Internet FTP servers.
- Printing and Security Features:
  - LPD: supports queued printing on a PC printer from a UNIX host.
  - LPR: allows Windows applications on a PC to transparently print to UNIX host printers.
  - XDMCP security.
  - Host Access Control List, restricting server access to authorized hosts.
  - User level access control.
  - Systems Administrators can restrict settings that users configure, etc.
- Font, Display, Keyboard, and Mouse Features:
  - X11R5 font support.
  - Full interactive support for all font naming and alias schemes.
  - Automatic font substitution.
  - Unlimited font size.
  - Hundreds of X fonts provided in Microsoft Windows format.
  - Display performance tuning.
  - 24-plane graphics board and TrueColor support (up to 16 million colors).
  - Three-button emulation on two-button mouse.
  - Graphical keyboard configurator, providing visual representation and editing of keyboard file mapping.
  - 17 international keyboard mappings.
- Network Transport Support:
  - eXceed 4 provides both Microsoft's VxD-based TCP/IP and SuperTCP for Windows. eXceed 4 for Windows also supports 22 other TCP/IP transports, plus DECnet, UNIXWare IPX/SPX, and all transports complying with Windows Sockets API.
- Hardware and Software Requirements on Your PC:
  - IBM compatible 80386, 80486, or Pentium-based PC.
  - Microsoft Windows 3.1 or higher.
  - Minimum 4 MB memory.
  - Hard disk drive: minimum 11 MB for storing software.
  - 1.44 MB disk drive.
  - Microsoft Windows supported mouse.
  - Color or analog monochrome monitor.
  - Microsoft supported graphics adapter.
  - TCP/IP transport provided with eXceed 4 for Windows, WinSock 1.1, or one of the many supported transports.

**B.3.2.1.3 Product Evaluation.** eXceed's setup program provides a Personal, User, Shared, or Copy installation. The differences were well-explained. The Personal option was selected, since that is the norm for a standalone PC. Installation was Windows-based and was easy to follow, although a longer install time was needed when compared to the other products.

eXceed supports many TCP/IP stacks and thus had no problem recognizing the TCP/IP stacks used in the evaluation. A number of networking tools and features are provided. The interface for eXceed was much more difficult to use compared to XoftWare/32 and PC-Xware.

The product successfully ran all GCCS applications with some minor tuning. For example, 100dpi fonts must be installed for the CAFMS applications and "preserve system colors" should not be selected since this crashed the DART TPFDD editor. The UCCS session manager banner could not be moved or iconized, thereby making the X console and Xterm windows difficult to manipulate as their banner bars remained underneath the UCCS session manager bar. This makes the GCCS applications much harder to use.

Table B-1 depicts the results of the evaluation of eXceed 4 for Windows.

**Table B-1. Evaluation Criteria of eXceed 4 Windows**

|                                                       |                                                                                                                           |
|-------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------|
| <b>Networking</b>                                     |                                                                                                                           |
| Provides support for many TCP/IP stacks?              | Supports most well known TCP/IP stacks.                                                                                   |
| <b>Features</b>                                       |                                                                                                                           |
| Are networking tools useful and valuable?             | Has the greatest number of tools, most could be provided by TCP/IP stack, but could be useful if users require the tools. |
| Are desktop tools useful and valuable?                | Yes, they help in configuration of product.                                                                               |
| <b>Installation</b>                                   |                                                                                                                           |
| Provides standard and custom installs?                | Has multiple install options, such as personal, shared, custom.                                                           |
| Were multiple installations needed of other packages? | No.                                                                                                                       |
| Did the X-Server find the existing TCP/IP stack?      | Yes, Window socket 1.1.                                                                                                   |
| Was X-Server easy to configure?                       | Yes.                                                                                                                      |
| Was is it easy to start X clients?                    | Yes, allowed icons to be built instead of using launch dialog.                                                            |
| <b>Performance</b>                                    |                                                                                                                           |
| Did clients start quickly?                            | Yes.                                                                                                                      |
| Was interactive performance acceptable?               | Yes, once speed controls were set to maximum (may depend on your hardware).                                               |

**Table B-1. Evaluation Criteria of eXceed 4 Windows (Cont.)**

| <b>Stability</b>                                        |                                                                                  |
|---------------------------------------------------------|----------------------------------------------------------------------------------|
| Did clients crash the server or suffer from X errors?   | Yes, caused DART to crash if preserve system colors is selected (see Table B-2). |
| Are enough winsockets available for many X windows?     | Yes, this is dependent on TCP/IP stack.                                          |
| <b>Documentation</b>                                    |                                                                                  |
| Was it complete and thorough?                           | Yes.                                                                             |
| Was information provided about supported TCP/IP stacks? | Yes.                                                                             |

### **B.3.2.2 XoftWare/32 for Windows**

#### **B.3.2.2.1 Product Overview**

**Vendor/Product:** AGE Logic Inc./XoftWare/32 for Windows 3.01

**Phone:** 619-455-8600

**Fax:** 619-597-6030

**Address:** 9985 Pacific Heights Blvd.  
San Diego, CA 92121

**B.3.2.2.2 Product Description.** XoftWare/32 for Windows provides 32-bit performance, X11R5 server technology, network enhancing utilities, remote access capabilities.

- **Main Server Features:**
  - 32-bit PC X-Server.
  - Windows based installation/configuration.
  - Iconized login and startup system.
  - Cut and paste tool for sharing information between UNIX and Microsoft Windows.
  - X11R5 compliance.
  - TrueColor support.
  - Single and multiple windowing modes.
  - Host based (Motif, OpenLook, etc.) or local window managers (you may utilize Windows as your local window manager).
  - Cascade X Window Focus Policy.
  - X style Panning.
  - Automatic font substitution.
  - Color Map reservation system.
- **Communications Features:**

Many start-up methods, including:

  - TELNET, REXEC, RSH, RLOGIN, XDMCP.
  - Support for local XDMCP Display Manager Chooser, presenting a list of hosts willing to manage the X display.

- Application start-up options, and X session drag-and-drop, point and click start-up of multiple X Windows, and non-X applications.
- Includes an icon library for custom icon installation; Transport Monitor provides visual feedback of transport activity.
- File Transfer and Management Features:
  - FTP supports graphical drag-and-drop file transfer and directory management.
  - Supports Active FTP connections.
  - Connection to Internet FTP servers.
- Printing Features:
  - Print Re-route enables networked users to re-direct multiple UNIX print jobs.
- Font, Display, Keyboard, and Mouse Features:
  - X11R5 font support.
  - Full interactive support for all font naming and alias schemes.
  - Automatic font substitution.
  - Display performance tuning.
  - 24-plane graphics board and TrueColor support (up to 16 million colors).
  - Three-button emulation on two-button mouse.
  - Graphical keyboard configurator, providing visual representation and editing of keyboard file mapping.
- Network Transport Support:
  - XoftWare/32 supports many other TCP/IP transports, plus DECnet, UnixWare IPX/SPX, and all transports complying with Windows Sockets API.
- Hardware and Software Requirements:
  - IBM compatible 80386, 80486, or Pentium-based PC.
  - Microsoft Windows 3.1 or higher.
  - Minimum 2 MB of extended memory.
  - Hard disk drive: minimum 6 MB for storing software.
  - 1.44 MB disk drive.
  - Microsoft Windows supported mouse.
  - Color or analog monochrome monitor.
  - Microsoft supported graphics adapter.
  - TCP/IP transport.

**B.3.2.2.3 Product Evaluation.** Installation of XoftWare/32 for Windows was the easiest of all the products tested. The Windows-based installation program was straightforward and easy to use. XoftWare/32 also had no problem determining the TCP/IP stack in use and worked well with both TCP/IP tested stacks. Documentation was good and easy to understand.

XoftWare/32 supports a full set of application start-up techniques, including Telnet, remote commands (rexec, rsh, and rlogin), and XDMCP.



Although XoftWare/32 provides no independent desktop, it does have easy-to-use tools to create icons that start remote X clients.

One major feature of XoftWare/32 is the ability to run a remote X Window manager simultaneously with MS Windows manager. This makes the use of MS Windows applications and X Windows applications much easier for the user. While not the most feature-rich X-Server tested, XoftWare/32 provides an uncomplicated product that should be easy to integrate and install at GCCS sites. This strategy has meant success for AGE, gaining them major customers and government agencies. AGE supplies the underlying software to other X-Servers sold by FTP Software; Spry Inc.; Distinct Corp.; and Walker, Richer, & Quinn (Reflection-X).

XoftWare/32 ran all GCCS applications tested except GSORTS 1.0. One major difference that XoftWare/32 provided over eXceed and PC-Xware was that the session manager banner can be moved or iconized if desired, thereby making X console and Xterm windows readily available to the user. This makes GCCS applications much easier to use and more manageable. Another difference is "preserve system colors" should not be toggled on so DART colors will display properly. If this option is selected toggled on, DART will work although the colors will not be correct.

Table B-2 depicts the evaluation criteria of XoftWare/32 for Windows.

**Table B-2. Evaluation Criteria of XoftWare/32 for Windows**

| <b>Networking</b>                                     |                                                                           |
|-------------------------------------------------------|---------------------------------------------------------------------------|
| Provides support for many TCP/IP stacks?              | Supports most well-known TCP/IP stacks; comes bundled with Novell TCP/IP. |
| <b>Features</b>                                       |                                                                           |
| Are networking tools useful and valuable?             | Provides just TELNET and FTP, which are easy to use.                      |
| Are desktop tools useful and valuable?                | Yes.                                                                      |
| <b>Installation</b>                                   |                                                                           |
| Provides standard and custom installs?                | Provides default and custom installs.                                     |
| Were multiple installations needed of other packages? | No.                                                                       |
| Did the X-Server find the existing TCP/IP stack?      | Yes, both Chameleon and Microsoft.                                        |
| Was X-Server easy to configure?                       | Yes, one of the easiest to use and configure.                             |

**Table B-2. Evaluation Criteria of XoftWare/32 for Windows (Cont.)**

|                                                         |                                                                     |
|---------------------------------------------------------|---------------------------------------------------------------------|
| Was is it easy to start X clients?                      | Yes, provided ability to make icons.                                |
| <b>Performance</b>                                      |                                                                     |
| Did clients start quickly?                              | Yes.                                                                |
| Was interactive performance acceptable?                 | Yes, one of the fastest.                                            |
| <b>Stability</b>                                        |                                                                     |
| Did clients crash the server or suffer from X errors?   | No.                                                                 |
| Are enough winsockets available for many X windows?     | Yes, depends on TCP/IP stack in use.                                |
| <b>Documentation</b>                                    |                                                                     |
| Was it complete and thorough?                           | Yes.                                                                |
| Was information provided about supported TCP/IP stacks? | Yes, but not comprehensive, except for Novell, which comes bundled. |

### **B.3.2.3 PC-Xware**

#### **B.3.2.3.1 Product Overview**

**Vendor/Product:** Network Computing Devices Inc./PC-Xware 2.01

**Point of Contact:**

**Phone:** 503-641-2200/800-PCX-WARE

**Fax:** 503-643-8642

**Address:** 9590 SW Gemini Dr.  
Beaverton, OR 97005

**Pricing:** \$545.00 single user, discounts available for multiple copies

**B.3.2.3.2 Product Description.** PC-Xware integrates UNIX and Windows on the PC in the Microsoft Windows environment. With Folder Tabs, users can navigate through PC-Xware's features to display UNIX graphic and character-based applications alongside local PC applications. PC-Xware lets users transfer UNIX files to their PC and print UNIX documents to a local printer. PC-Xware features a 32-bit PC X-Server, Telnet for VT320 terminal emulation, an integrated 32-bit VxD TCP/IP stack, support for 15 other TCP/IP protocols including WinSock, and XRemote for serial line connections. To help administer the software, PC-Xware includes site installation capabilities, and remote diagnostic and configuration control.

- Main Server Features:

- X11R5 compliance.
- Simple Image Extension.
- XDM protocol.
- 32-bit PC X-Server.
- Windows-based installation/configuration.
- Iconized login and startup system.
- Cut and paste tool for sharing information between UNIX and Microsoft Windows.
- TrueColor support.
- Single and multiple windowing modes.
- Host-based (Motif, OpenLook, etc.) or local window managers (you may utilize Windows as your local window manager).
- X style Panning.
- Automatic font substitution.
- Color Map reservation system.
- Communications Features:  
Many start-up methods, including:
  - TELNET, REXEC, RSH, RLOGIN, XDMCP.
  - Support for local XDMCP Display Manager Chooser, presenting a list of hosts willing to manage the X display.
  - Includes an icon library for custom icon installation.Transport Monitor provides visual feedback of transport activity.
- File Transfer and Management Features:
  - File server installation.
  - Remote configuration.
  - SNMP with NCD MIB extensions for X.
- Printing Features:
  - Print Re-route enables networked users to re-direct multiple UNIX print jobs.
- Font, Display, Keyboard, and Mouse Features:
  - X11R5 font support.
  - Full interactive support for all font naming and alias schemes.
  - Automatic font substitution.
  - Display performance tuning.
  - 24-plane graphics board and TrueColor support (up to 16 million colors).
  - Three-button emulation on two-button mouse.
- Network Transport Support:
  - Includes VxD TCP/IP kernel.
  - Includes XRemote serial protocol.
  - Supports 15 other TCP/IP stacks, including WinSock.
  - DECnet via support of DEC Pathworks.
- Hardware and Software Requirements:
  - IBM compatible 80386, 80486, or Pentium-based PC.
  - Microsoft Windows 3.1 or higher.
  - Minimum 6 MB of extended memory.

- Hard disk drive: minimum 7 MB for storing software.
- 1.44 MB disk drive.
- Microsoft Windows supported mouse.
- Color or analog monochrome monitor.
- Microsoft supported graphics adapter.
- TCP/IP transport.

**B.3.2.3.3 Product Evaluation.** PC-Xware installation was easy and provided the most user-friendly interface of all the packages. PC-Xware comes bundled with its own TCP/IP stack from NCD; however, the product had no trouble determining the stack in use for the test. It worked well with both Chameleon and Microsoft's TCP/IP stack.

Two features of PC-Xware that are worth mentioning are remote management and monitoring. These features allow users to view TCP/IP use and resources while the UCCS desktop was running. Product documentation on how to use and setup the product was good.

PC-Xware ran all GCCS applications tested, except GSORTS 1.0. One major difference that PC-Xware could not provide over XoftWare/32 and Reflection-X was the UCCS session manager banner could not be moved or iconized, thereby making X console and Xterm windows difficult to manipulate. This makes GCCS applications much harder to use.

Table B-3 depicts the evaluation criteria of PC-Xware.

**Table B-3. Evaluation Criteria of PC-Xware**

| <b>Networking</b>                                     |                                                                                |
|-------------------------------------------------------|--------------------------------------------------------------------------------|
| Provides support for many TCP/IP stacks?              | Yes, supports most well known TCP/IP stacks, comes bundled with NCD own stack. |
| <b>Features</b>                                       |                                                                                |
| Are networking tools useful and valuable?             | Yes, but has only TELNET and FTP.                                              |
| Are desktop tools useful and valuable?                | Yes, the most user-friendly.                                                   |
| <b>Installation</b>                                   |                                                                                |
| Provides standard and custom installs?                | Yes.                                                                           |
| Were multiple installations needed of other packages? | No.                                                                            |
| Did the X-Server find the existing TCP/IP stack?      | Yes, both Chameleon and Microsoft.                                             |
| Was X-Server easy to configure?                       | Yes.                                                                           |

**Table B-3. Evaluation Criteria of PC-Xware (Cont.)**

|                                                         |                                                               |
|---------------------------------------------------------|---------------------------------------------------------------|
| Was is it easy to start X clients?                      | Yes, icons can be built instead of using startup dialog.      |
| <b>Performance</b>                                      |                                                               |
| Did clients start quickly?                              | Yes.                                                          |
| Was interactive performance acceptable?                 | Yes, performed very equal to other when set at highest speed. |
| <b>Stability</b>                                        |                                                               |
| Did clients crash the server or suffer from X errors?   | No.                                                           |
| Are enough winsockets available for many X Windows?     | Yes, depends on TCP/IP stack used.                            |
| <b>Documentation</b>                                    |                                                               |
| Was it complete and thorough?                           | Yes.                                                          |
| Was information provided about supported TCP/IP stacks? | Yes.                                                          |

#### **B.3.2.4 Reflection-X**

##### **B.3.2.4.1 Product Overview**

**Vendor/Product:** Walker Richer & Quinn, Inc./Reflection X 4.1

**Point of Contact:** Sales

**Phone:** 800-872-2829

**Fax:**

**Address:** 1500 Dexter Avenue North

P.O. Box 31876

Seattle, WA 98103-1876

**Pricing:** Single-user; discounts available for multiple copies

**B.3.2.4.2 Product Description.** Version 4.1 of Reflection-X delivers TCP/IP connections for Windows, DECnet support, Windows Management, TrueColor support and many other features to help assist users in PC-to-UNIX connectivity. Reflection-X is based on AGE's XoftWare/32.

- Main Server Features:
  - 32-bit PC X-Server.
  - Windows-based installation/configuration.
  - Iconized login and startup system.
  - Cut and paste tool for sharing information between UNIX and Microsoft Windows.
  - X11R5 compliance.

- TrueColor support.
- Single and multiple windowing modes.
- Host-based (Motif, OpenLook, etc.) or local window managers (you may utilize Windows as your local window manager).
- Cascade X Window Focus Policy.
- X style Panning.
- Automatic font substitution.
- Color Map reservation system.
- Communications Features:  
Many start-up methods, including:
  - TELNET, REXEC, RSH, RLOGIN, XDMCP.
  - Support for local XDMCP Display Manager Chooser, presenting a list of hosts willing to manage the X display.
  - Application start-up options.
  - Includes an icon library for custom icon installation.
- File Transfer and Management Features:
  - FTP supports graphical drag-and-drop file transfer and directory management.
  - Supports Active FTP connections.
  - Connection to Internet FTP servers.
- Printing Features:
  - Print Re-route enables networked users to re-direct multiple UNIX print jobs.
- Font, Display, Keyboard, and Mouse Features:
  - X11R5 font support.
  - Automatic font substitution.
  - Display performance tuning.
  - 24-plane graphics board and TrueColor support (up to 16 million colors).
  - Three-button emulation on two-button mouse.
- Network Transport Support:
  - Includes VxD TCP/IP kernel.
  - Includes XRemote serial protocol.
  - Supports other TCP/IP stacks, including WinSock.
- Hardware and Software Requirements:
  - IBM compatible 80386, 80486, or Pentium-based PC; (80486 or better is recommended).
  - Microsoft Windows 3.1 or higher.
  - Minimum 2 MB of extended memory (8 MB recommended).
  - Hard disk drive: minimum 9.5 MB for storing software.
  - 1.44 MB disk drive.
  - Microsoft Windows supported mouse.
  - Color or analog monochrome monitor.
  - Microsoft supported graphics adapter.
  - TCP/IP transport.

**B.3.2.4.3 Product Evaluation.** Installation of Reflection-X for Windows was straightforward, but very lengthy. Reflection-X had no

problem determining the TCP/IP stack in use, and worked well with both tested TCP/IP stacks. Documentation was good but not very well organized.

Reflection-X supports a full set of application start-up techniques, including Telnet, remote commands (rexec, rsh, and rlogin), and XDMCP. The interface to setting up the software is more difficult than most of the other packages. The large number of dialog boxes can become confusing.

Reflection-X ran all GCCS applications tested except GSORTS 1.0. One major difference that Reflection-X provided over eXceed and PC-Xware was the UCCS session manager banner can be moved or iconized, thereby making X console and Xterm windows available to the user with a click of the mouse button. The underlying software for Reflection-X is supplied by XoftWare/32. Table B-4 depicts the evaluation criteria of Reflection-X.

**Table B-4. Evaluation Criteria of Reflection-X**

|                                                       |                                                                     |
|-------------------------------------------------------|---------------------------------------------------------------------|
| <b>Networking</b>                                     |                                                                     |
| Provides support for many TCP/IP stacks?              | Yes, most well-known TCP/IP stacks.                                 |
| <b>Features</b>                                       |                                                                     |
| Are networking tools useful and valuable?             | Yes, but has only TELNET and FTP.                                   |
| Are desktop tools useful and valuable?                | Yes.                                                                |
| <b>Installation</b>                                   |                                                                     |
| Provides standard and custom installs?                | Yes.                                                                |
| Were multiple installations needed of other packages? | No.                                                                 |
| Did the X-Server find the existing TCP/IP stack?      | Yes, both Chameleon and Microsoft.                                  |
| Was X-Server easy to configure?                       | Yes.                                                                |
| Was is it easy to start X clients?                    | Not as easy as other products, had a lot to select in dialog boxes. |
| <b>Performance</b>                                    |                                                                     |
| Did clients start quickly?                            | Yes.                                                                |
| Was interactive performance acceptable?               | Yes, with speed turned up to maximum.                               |
| <b>Stability</b>                                      |                                                                     |

**Table B-4. Evaluation Criteria of Reflection-X (cont.)**

|                                                         |                                    |
|---------------------------------------------------------|------------------------------------|
| Did clients crash the server or suffer from X errors?   | No.                                |
| Are enough win sockets available for many X Windows?    | Yes, depends on TCP/IP stack used. |
| <b>Documentation</b>                                    |                                    |
| Was it complete and thorough?                           | Yes, but not very well organized.  |
| Was information provided about supported TCP/IP stacks? | Yes.                               |

#### **B.4 TCP/IP Candidate Products**

**B.4.1 Summary of Findings.** The Microsoft TCP/IP stack, using VxD technology, worked with all the PC X-Servers reviewed and provided 256 winsockets. Because this product lacks NFS and other network tools, and requires Microsoft Windows for Workgroups 3.11, it is a poor choice for GCCS. Chameleon/NFS is extensive and friendly and provides many network tools that GCCS could use, both now and in the future. It is also a very solid product and provides 128 winsockets through use of DLL technology. Some early TCP/IP products, such as PC-NFS 5.1, were based on Terminate and Stay Resident technology and are inadequate for GCCS.

#### **B.4.2 Product Reviews**

##### **B.4.2.1 Chameleon/NFS**

##### **B.4.2.1.1 Product Overview**

**Vendor/Product:** NetManage Inc./ChameleonNFS 4.0  
**Point of Contact:** Tim Buckler  
**Phone:** 408-973-7171  
**Fax:** 408-257-6405  
**Address:** 20823 Stevens Creek Blvd.  
 Cupertino, CA 95014  
**Pricing:** \$495, quantity discounts available

**B.4.2.1.2 Product Description.** Chameleon/NFS provides Microsoft Windows users with communications applications for inter-networking in a multi-vendor network environment. TCP/IP has emerged as the most common networking standard for linking heterogeneous networks. TCP/IP protocol and applications are used by corporations to join their diverse computers together from Windows PCs to UNIX workstations, to Macintoshes, to VAXes, to AS400s, to IBM mainframes. TCP/IP is also the protocol of the Internet, the world's largest network. The industry TCP/IP standards WinSock and WinSNMP are based on NetManage specifications.



- Terminal Emulation

Chameleon provides Telnet, TN3270 and TN5250 terminal emulation, a Visual Script Editor and Player applications for automating terminal emulation sessions with a graphical Windows front end.

The Telnet application allows users to log into any other networked computer with a Telnet server, such as a UNIX workstation or a VAX. Terminal emulations include VT52, VT100, VT220, TVI 950 and 955. Telnet provides features such as "capture to file" and a button pad.

The NetManage TN3270 provides 3270 emulation, including support for models 2, 3, 4, and 5, with extended attributes, HLLAPI interface, Hotspots, IND\$file transfer and an IBM status line.

All emulations provide logging with playback, printing, copy and paste, scripting, user-definable colors and fonts, and drag-and-drop keyboard remapping.

- Client/Server File and Printer Sharing

NetManage provides a range of TCP/IP-based file and print sharing tools. File transfer and sharing can be done with FTP, TFTP, or NFS. All three applications are provided as both client and server. The NetManage FTP client provides users with a point-and-click interface. Connection profiles can be set up in advance for sites that are accessed frequently. Navigation through directory structures can be done entirely with a mouse. Users can create or rename remote directories, view, print, and rename files or use drag-and-drop to transfer files directly to the PC hard disk. Chameleon's FTP Server allows Windows users to make their files available to any other host. Peer-to-peer connections can be made between PCs as needed with full name and password security. Printing can be done with either LPR/LPD or PCNFSD. This set of options allows PCs to send print jobs to either UNIX systems or other PCs while simultaneously allowing UNIX workstations to print to a PC printer.

- NFS Client/Server

NetManage's NFS provides client/server functionality for the PC. You can share files and directories with any other NFS system including UNIX, IBM, DEC, Macintosh, and other PCs.

With NFS, it is possible to execute programs over the network or run applications locally while transparently storing data on a network server. The NFS client can support as many as 24 network drives. All functionality is integrated into the Windows File Manager, so accessing a remote drive is as simple as pointing to a disk icon and clicking. All remote

systems appear as directories and files in File Manager. You can even transfer files between two remote systems from your PC.

- Electronic Mail

Chameleon's NEWTMail application allows users to create, send, receive, reply, forward, and save mail messages via Windows dialogs. Mail users can create their own personal address books, foldering system, and write automatic rules for filtering and filing mail. Users can send multiple attachments such as a spreadsheet using MIME (Multi-purpose Internet Mail Extensions) as easily as dragging and dropping files into their mail message.

The mail application supports both Simple Mail Transfer Protocol (SMTP) running as both client and mail server. Chameleon users can create their own mail network or integrate with existing enterprise mail systems such as Microsoft Mail or cc:Mail via an SMTP gateway, or send directly to UNIX mail. Chameleon's PhoneTag application allows users to send, receive, and file phone messages electronically.

- Internet Access Tools

Chameleon includes a Gopher Client, NEWTNews Internet News Reader, and WhoIs. NetManage's Gopher search tool lets users find information using a keyword search, and has an interface that makes the Internet look like a directory system on a local PC.

NEWTNews allows users to subscribe to Internet news groups. It is possible to read, post, and follow up messages. Messages can be sorted by date, subject, or sender to simplify finding a particular message. The WhoIs application allows the user to identify people and resources on the Internet.

- Network Communications and Utilities

Chameleon includes applications necessary to facilitate the operation and administration of the organization's network. These include NetRoute, a software-only static IP router that supports Ethernet, Token Ring, FDDI, and serial line. Other applications in this category include a Domain Name Server (DNS) for directory services, ping echo locate, finger user information, and a Bootp client. Users can track and display all Network Statistics for the network interface including ARP, IP, ICMP, UDP, and TCP protocols.

Every Chameleon comes with an extensible SNMP Agent that runs in the background and gathers information about the network, allowing a system administrator to monitor the health of the

network and each workstation from a centralized network management station. The SNMP agent features multiple Management Information Bases (MIBs), including MIB\_II, Windows, DOS, Workstation, and RMON.

**B.4.2.1.3 Product Evaluation.** Chameleon/NFS was very easy to install. Chameleon automatically wrote to all configuration files during installation and did not require modification to configuration files after plugging in the necessary information such as IP address. Chameleon/NFS does not require any virtual device drivers. See Appendix D for a more detailed discussion on TCP/IP implementations. Table B-5 lists Chameleon TCP/IP attributes.

Chameleon/NFS transfer speeds were above average but slower than the Microsoft TCP/IP stack. Chameleon/NFS worked with all PC X-Server packages tested with no problems encountered. Chameleon/NFS only provides 128 winsockets, but this proved to be more than enough for the GCCS applications tested (see Appendix C for a detailed description of driver implementations).

The main strength of Chameleon/NFS is the suite of Windows tools for network access, such as FTP, Internet News Reader (which could prove useful for WIN Teleconferencing) e-mail, NFS client, NFS server, and DNS client and server. NetManage devotes one chapter to each Windows application included with plenty of screen shots, diagrams, and charts to help make the documentation understandable and easy to follow.

**Table B-5. TCP/IP for PC Attributes**

|                              | Chameleon/NFS | Microsoft VxD<br>WinSock |
|------------------------------|---------------|--------------------------|
| <b>Network Interfaces</b>    |               |                          |
| Ethernet                     | •             | •                        |
| Token Ring                   | •             | •                        |
| FDDI                         | •             |                          |
| X.25                         |               |                          |
| <b>Driver Implementation</b> |               |                          |
| VxD, TSR, DLL                | DLL           | VxD                      |
| Win Sockets<br>Supported     | 128           | 256                      |
| <b>Driver Type</b>           |               |                          |
| Packet Driver                |               |                          |
| NDIS                         | •             |                          |
| ODI                          | •             |                          |
| SLIP                         | •             |                          |
| PPP                          | •             |                          |
| <b>TCP/IP Servers</b>        |               |                          |

**Table B-5. TCP/IP for PC Attributes (cont.)**

|                         | <b>Chameleon/NFS</b> | <b>Microsoft VxD<br/>WinSock</b> |
|-------------------------|----------------------|----------------------------------|
| DNS                     | MS Windows           |                                  |
| SMTP                    |                      |                                  |
| ftp                     | MS Windows           | MS Windows                       |
| NFS                     | MS Windows           |                                  |
| Print Server            | MS Windows           |                                  |
| Tftp                    | MS Windows           |                                  |
| Finger                  | MS Windows           |                                  |
| Time                    |                      |                                  |
| <b>Talk</b>             |                      |                                  |
| Telnet                  | MS Windows           | MS Windows                       |
| ftp                     | MS Windows           | MS Windows                       |
| SMTP Mail               | MS Windows           |                                  |
| POP2/3 Mail             | MS Windows           |                                  |
| Usenet News             | MS Windows           |                                  |
| Finger                  | MS Windows           |                                  |
| Talk                    | MS Windows           |                                  |
| NFS                     | MS Windows           |                                  |
| whois                   | MS Windows           |                                  |
| LPR                     |                      |                                  |
| LPQ                     |                      |                                  |
| LPRM                    |                      |                                  |
| REXEC                   |                      |                                  |
| RSH                     |                      |                                  |
| RCP                     |                      |                                  |
| Rlogin                  | MS Windows           |                                  |
| Tftp                    | MS Windows           |                                  |
| TN 3270                 | MS Windows           |                                  |
| <b>IP Network Tools</b> |                      |                                  |
| nslookup                |                      |                                  |
| Ping                    | MS Windows           |                                  |
| Traceroute              |                      |                                  |
| SNMP Agent              | MS Windows           |                                  |
| Statistics              | MS Windows           |                                  |

#### **B.4.2.2 Microsoft VxD 32 TCP/IP**

##### **B.4.2.2.1 Product Overview**

**Vendor/Product:** Microsoft TCP/IP-32 for Windows for Workgroups  
**Point of Contact:** Sales  
**Phone:** 1-800-426-9400  
**Fax:** 1-800-727-3351  
**Address:** Microsoft Corporation  
One Microsoft Way  
Redmond, WA 98052-6399  
**Pricing:** Free; Requires Windows for Workgroups 3.11

**B.4.2.2.2 Product Description.** Microsoft TCP/IP-32 for Windows for Workgroups 3.11 includes Microsoft's latest NDIS 3 protocol stack supporting Windows for Workgroups 3.11. Microsoft TCP/IP-32 includes a number of diagnostic utilities, support for DHCP automatic configuration, and industry standard Windows Sockets support for third party and public domain TCP/IP applications such as NCSA Mosaic. This stack requires Windows for Workgroups 3.11, and cannot execute outside of Windows (e.g., in MS-DOS before running Windows for Workgroups).

Most Windows Sockets applications should work fine under the Microsoft VxD release. Microsoft VxD performance compared to other stacks is very good.

The Microsoft VxD WinSock is focused on providing high-performance VxD transport functionality. Since the stack supports the Windows Sockets API, public domain and commercial Windows Sockets applications are compatible with this product. Please see Appendix D for a more detailed discussion on VxD technology. NFS support is not planned for this product release.

**B.4.2.2.3 Product Evaluation.** The Microsoft TCP/IP stack installed easily and worked well with all PC X-Servers. The stack provides 256 winsockets, which is more than enough for GCCS. The product does not come with any documentation in the form of a manual. The Microsoft TCP/IP stack comes only with a crude form of Telnet and FTP that are useable, but less capable than other products, including some public domain products.

The performance was slightly faster than that of Chameleon/NFS. (Appendix C contains a graphical comparison of the speed of the two stacks.) The Microsoft TCP/IP stack does not support NFS, which means a third party product would have to be used. Table B-5 provides the product's TCP/IP attributes.

## B.5 PC X-Server Attributes/Requirements/Features

Table B-6 depicts the PC X-Server attributes and requirements of the candidate products.

**Table B-6. PC X-Server Attributes and Requirements**

|                                                  | eXceed 4.0         | PC-Xware 2.0         | XoftWare/32<br>3.1                    | Reflectio<br>n-X                         |
|--------------------------------------------------|--------------------|----------------------|---------------------------------------|------------------------------------------|
| Minimum CPU                                      | 80386 (80486)      | 80386 (80486)        | 80386 (80486)                         | 80386<br>(80486)                         |
| Memory<br>Requirements                           | 4MB (6MB)          | 6MB (8MB)            | 4MB (8MB)                             | 4MB (8MB)                                |
| Minimum Disk Space<br>Required                   | 11MB               | 7MB                  | 13MB for<br>default<br>install        | 9.5MB                                    |
| Technical Support                                | Yes                | Yes                  | Yes                                   | Yes                                      |
| Serial Support                                   | Xpress             | XRemote              | SLIP/PPP                              | SLIP/PPP<br>if stack<br>supports<br>this |
| Window Manager<br>Options                        | HWM, MS<br>Windows | MS Windows,<br>NCDWM | MS Windows or<br>X Windows<br>manager | MS<br>Windows<br>or X<br>Windows         |
| Supports host-<br>based remote<br>window manager | Motif,<br>OpenLook | Motif,<br>OpenLook   | Motif,<br>OpenLook                    | Motif,<br>OpenLook                       |
| Font Manager<br>Support                          | Yes                | Yes                  | Yes                                   | Yes                                      |
| Additional<br>Resources Required                 |                    |                      |                                       |                                          |
| X Windows System<br>Supported                    | X11R5              | X11R5                | X11R5                                 | X11R5                                    |
| Backing store/save<br>Supported                  | Yes                | Yes                  | Yes                                   | Yes                                      |
| Mouse Required                                   | Yes                | Yes                  | Yes                                   | Yes                                      |
| MS Windows 3.1 or<br>greater Required            | Yes                | Yes                  | Yes                                   | Yes                                      |
| DOS version<br>Required                          | 5.0 or greater     | 5.0 or<br>greater    | 3.1 or<br>greater                     | 3.1 or<br>greater                        |

Table B-7 depicts the PC X-Server features of the candidate products.

**Table B-7. PC X-Server Features of the Candidate Products (Cont.)**

| <b>Features</b>                         | <b>eXceed 4<br/>Windows</b>   | <b>XoftWare/32</b>  | <b>PC-Xware</b>      | <b>Reflection-X</b>        |
|-----------------------------------------|-------------------------------|---------------------|----------------------|----------------------------|
| <b>Main Server:</b>                     |                               |                     |                      |                            |
| X11R5 compliance                        | yes                           | yes                 | yes                  | yes                        |
| Mode                                    | 32-bit                        | 32-bit              | 32-bit               | 32-bit                     |
| Control panel-style configuration       | yes                           | yes                 | yes                  | yes                        |
| Backing store/save unders               | yes                           | yes                 | yes                  | yes                        |
| Local Window Manager                    | hwm & Windows                 | Windows & X Windows | NCDWM, Windows       | Windows & X Windows        |
| Remote Window Manager (Motif, OpenLook) | yes                           | yes                 | yes                  | yes                        |
| Launch Pad                              | yes                           | yes                 | yes                  | yes                        |
| Vitural Desktop                         | yes                           | no                  | no                   | no                         |
| Xtrace (debugging)                      | yes                           | yes                 | no                   | no                         |
| Scripting Language                      | yes<br>(proprietary)          | no                  | yes                  | no                         |
| <b>Communications:</b>                  |                               |                     |                      |                            |
| TELNET                                  | yes                           | yes                 | yes                  | yes                        |
| RLOGIN                                  | yes                           | yes                 | yes                  | yes                        |
| RSH                                     | yes                           | yes                 | yes                  | yes                        |
| REXEC                                   | yes                           | yes                 | yes                  | yes                        |
| Program starter - point & click         | yes                           | yes                 | yes                  | yes                        |
| UNIX/DOS file transfer                  | yes (Drag & Drop)             | yes (Drag & Drop)   | yes                  | yes                        |
| Local Printing                          | yes                           | yes                 | yes                  | yes                        |
| Copy & paste between PC & Host          | yes                           | yes                 | yes                  | yes                        |
| Transport Monitor                       | yes                           | yes                 | no                   | yes                        |
| Serial Connection support               | optional                      | yes                 | yes                  | optional                   |
| TCP/IP software included                | yes<br>(SuperTCP & Microsoft) | yes (Novell)        | yes (NCD integrated) | yes<br>(Reflection TCP/IP) |
| <b>Security:</b>                        |                               |                     |                      |                            |
| X11R5-XDMCP security                    | yes                           | yes                 | yes                  | no                         |

**Table B-7. PC X-Server Features of the Candidate Products (Cont.)**

| <b>Features</b>                                     | <b>eXceed 4<br/>Windows</b> | <b>XoftWare/32</b> | <b>PC-Xware</b>          | <b>Reflection-X</b> |
|-----------------------------------------------------|-----------------------------|--------------------|--------------------------|---------------------|
| Access Control                                      | yes                         | yes                | yes                      | no                  |
| <b>Fonts:</b>                                       |                             |                    |                          |                     |
| X11R5-font server,<br>scalable fonts                | yes                         | yes                | yes                      | yes                 |
| Auto substitution                                   | yes                         | yes                | yes                      | yes                 |
| Fonts: 75dpi, 100dpi,<br>HP, IBM, DEC, Misc         | yes                         | yes                | yes                      | yes                 |
| Font compiler (.bdf,<br>.pcf)                       | yes                         | yes                | yes                      | yes                 |
| <b>Display/Keyboard/Mouse:</b>                      |                             |                    |                          |                     |
| PseudoColor,<br>StaticColor,<br>GrayColor,TrueColor | yes                         | yes                | yes                      | yes                 |
| International keyboard<br>mapping included          | yes                         | yes                | yes                      | yes                 |
| Keyboard configuration<br>(graphical)               | yes                         | yes                | yes                      | yes                 |
| 3-button emulation on<br>2-button mouse             | yes                         | yes                | yes                      | yes                 |
| Concurrent Window<br>Managers                       | yes                         | yes                | yes                      | no                  |
| <b>Supported Network Transports:</b>                |                             |                    |                          |                     |
| Microsoft VxD 32<br>TCP/IP 3.11a                    | yes                         | yes                | yes                      | yes                 |
| Sun PC-NFS (Version<br>3.01 or higher)              | yes                         | yes                | yes                      | yes                 |
| 3Com 3+Open TCP                                     | yes                         | yes                | yes                      | yes                 |
| AT&T STARLAN                                        | no                          | no                 | no                       | no                  |
| AT&T StarGROUP                                      | no                          | no                 | no                       | no                  |
| DEC PATHWORKS for DOS<br>DECnet                     | yes                         | yes                | yes                      | yes                 |
| DEC PATHWORKS for DOS<br>TCP/IP                     | yes                         | yes                | yes                      | yes                 |
| Microsoft LAN Manager<br>TCP/IP                     | yes                         | yes                | yes                      | yes                 |
| Novell IPX/SPX                                      | yes                         | yes                | yes                      | yes                 |
| SuperTCP for Windows                                | yes                         | yes                | yes (not<br>Version 4.0) | Yes                 |



| Features                         | eXceed 4<br>Windows | XoftWare/32 | PC-Xware | Reflectio<br>n-X |
|----------------------------------|---------------------|-------------|----------|------------------|
| PC/TCP                           | yes                 | yes         | yes      | yes              |
| Chameleon/NFS TCP/IP             | yes                 | yes         | yes      | yes              |
| <b>Performance Optimization:</b> |                     |             |          |                  |
| Graphics performance<br>tuning   | yes                 | yes         | yes      | yes              |
| System resource usage<br>tuning  | yes                 | yes         | yes      | yes              |

## B.6 PCs-to-UNIX Connections: an Overview

**B.6.1 Desktop to Enterprise Connections.** Terminal access to enterprise-wide resources can be an inexpensive option, but it does not take advantage of the computing power on the desktop. Rather, there is a middle road, one that many organizations are finding most appealing. Today's client/server networking technologies are able to link PCs and Macintoshes to and through UNIX-based servers, providing access to enterprise-wide service while still offering users the personal freedom of applications for the desktop.

**B.6.2 TCP/IP Driver Implementations.** The PC-to-UNIX connection begins with a common network data-transmission protocol: TCP/IP. It's the standard for UNIX and is gaining popularity in the PC world. TCP/IP does not come naturally to PC systems. A "stack" of protocols that interface to the network driver to process IP, TCP, and UDP packets is needed. Keeping this in mind, we can look at the different implementations of TCP/IP stacks from vendors.

**B.6.3 TSR Implementation.** A Terminate and Stay Resident (TSR) program is one that loads into memory upon execution and then returns a DOS prompt, allowing the user to perform other tasks. The TSR remains active and occupies a portion of memory until it is either manually unloaded or removed by another action, such as rebooting the PC. For example, if a user activates a TSR program from the DOS prompt and then starts Microsoft Windows and accesses a spreadsheet application, the DOS TSR is still active in memory and running, even though the user is in a Windows application.

A TSR resides in real mode addressable DOS memory. Real mode addressable memory is the memory between 0 K and 1024 K (or 1 MB) that is typically used for loading device drivers and applications. This memory is comprised of the conventional memory area (0 K to 640 K) and the upper memory area (640 K to 1024 K). The upper memory area can consist of expanded memory (EMS) and upper memory (UMB) blocks.

The main concern with a Windows network protocol stack implemented as a TSR is that it uses a portion of real mode memory. Depending on the size and complexity of the program, little or no memory may be available for other applications. A TSR is a good implementation for DOS-based

protocols and a reliable, proven architecture for users who prefer to network primarily through DOS.

**B.6.4 DLL Implementation.** A Windows Dynamic Link Library (DLL) is only active when Windows is running. A DLL loads into memory only when an application needs the services the DLL provides. DLLs are "dynamically" loaded and unloaded as needed by Windows. When the application no longer needs the DLL's services, it gets unloaded automatically by Windows. For example, a user starts Windows and starts a remote login application - since that application requires the services of the DLL, the DLL is dynamically loaded by the Windows Scheduler. When the user finishes the remote login session and closes that application, Windows automatically unloads the DLL. A DLL implementation enables efficient use of system resources since it has the ability to dynamically load and unload when its services are needed.

However, a DLL is not free from the constraints of operating in real mode memory addressing. Windows "fixes" interrupt-driven DLL network protocol stacks into low memory (conventional memory). Windows-controlled memory is used to buffer (store) data and execute network code when interrupts occur. Implementing a network protocol stack as a DLL is a short-term solution for a Windows 3.0 or 3.1 environment. But what about companies that want to network in both DOS and Windows, and take advantage of future 32-bit Windows releases?

**B.6.5 The VxD Alternative.** A VxD architecture is Microsoft's recommended method for implementing network protocol stacks. VxD technology provides the overall best way to implement network protocol stacks within Windows: it takes full advantage of 386/486 architecture, it is written as a 32-bit module, and because it operates at the same level of priority as the operating system, it provides superior performance and faster response time to applications. Applications written as 32-bit implementations can talk through a 32-bit API directly to the VxD, without needing to go through a 32-bit to 16-bit conversion, which reduces performance.

There are several performance advantages that a Windows VxD protocol stack has in comparison to a TSR and DLL. Within Windows, a VxD provides simultaneous network support to Windows applications as well as network applications initiated from within a Windows DOS box. A TSR also offers this capability but, as previously mentioned, it lacks the ability to dynamically load or unload. In addition, a TSR can occupy a significant portion of memory depending on the size of the program. The VxD itself requires a very small portion of conventional memory for buffering information received from the network; however, the amount of conventional memory the VxD occupies is significantly less than its TSR or DLL counterparts, since it is only a buffer for network packets without any actual code.

A VxD also has some significant advantages over a DLL. First, a DLL implementation is limited because it does not support network applications initiated from a Windows DOS box. Also, a VxD has improved performance over a DLL because it operates at the same level of priority as the operating system. When a network protocol stack handles packets,

a VxD implementation will provide faster response time than a DLL. For end users, this means faster performance for both network applications and Windows.

**B.6.6 Microsoft's Recommendation for the Future: VxD.** A VxD architecture is Microsoft's recommendation for implementing network protocol stacks in Windows 3.1 and future versions. Microsoft also highly recommends a protected mode device driver. The NDIS v3.0 specification defines a method by which network implementations built-in protected mode can interface to protected mode drivers. Microsoft, through Windows for Workgroups v3.11, has released the protected mode device drivers defined in the NDIS v3.0 specification.

The combination of an NDIS v3.0 device driver and a VxD gives the user a complete protected mode network stack. This protected mode stack solves most of the traditional memory consumption issues that TSRs and DLLs present us with, and makes the amount of conventional memory that a network stack occupies almost non-existent.

**B.6.7 Summary.** A VxD is clearly the way that future Windows network protocol stacks will be implemented. VxD technology provides users with the ability to be aligned for future 32-bit versions. The advantages a VxD brings to users include:

- 32-bit technology that operates at the same priority level as the operating system and makes full use of a PC's 386/486 architecture.
- Superior performance for network applications.
- The fastest network protocol stack implementation in the marketplace.
- The smallest possible conventional memory use.
- No need for a memory manager.
- State-of-the-art technology that is well aligned for future operating systems and Microsoft Windows releases.

|                                             | TSR | DLL | VxD |
|---------------------------------------------|-----|-----|-----|
| Does not consume any DOS memory             |     | •   | •   |
| Capable of Windows memory allocation        |     | •   | •   |
| Offers protected mode                       |     | •   | •   |
| Has 32-bit code design                      |     |     | •   |
| Provides quick network response             | •   |     | •   |
| Supports DOS programs/NFS from command line | •   |     |     |
| Supports DOS programs/NFS from DOS window   | •   |     | •   |

|                               | TSR | DLL | VxD |
|-------------------------------|-----|-----|-----|
| Supports Windows programs/NFS | •   | •   | •   |

A VxD implementation will help meet some of the future challenges that companies using networks face. For those companies who want to migrate to future versions of Windows and keep up with networking technology, a VxD will soon become the preferred method for protocol stack implementation.

## APPENDIX C. MSQL DATABASE ADMINISTRATION GUIDE

### C.1 Introduction

Mini Structured Query Language (SQL), or mSQL, is a lightweight database engine designed to provide fast access to store data with low memory requirements. As its name implies, mSQL offers a subset of SQL as its query interface. Although it only supports a subset of SQL (no views, subqueries, etc.), everything it supports is in accordance with the American National Standard's Institute (ANSI) SQL specification. The mSQL package includes the database engine, a terminal "monitor" program, a database administration program, a schema viewer, and a C language API. The API and the database engine have been designed to work in a client/server environment over a TCP/IP network.

### C.2 Mini SQL Specification

The mSQL language offers a significant subset of the features provided by ANSI SQL. It allows a program or user to store, manipulate, and retrieve data in table structure. It does not support relational capabilities such as table joins, views, or nested queries. Although it does not support all the relational operations defined in the ANSI specification, it does provide the capability of "joins" between multiple tables.

The definitions and examples below depict mSQL key words. (Although they are provided here in upper case, no such restriction is placed on the actual queries).

**C.2.1 The Create Clause.** The create clause as supported by mSQL can only be used to create a table. It cannot be used to create other definitions such as views. It should also be noted that there can only be one primary key field defined for a table. Defining a field as a key generates an implicit "not null" attribute for the field.

```
CREATE TABLE table_name(col_name col_type [not null|primary key]
 [,col_name col_type [not null|primary key]]**)
```

For example:

```
CREATE TABLE emp_details
 first_name char(15) not null,
 last_name char(15) not null,
 dept char(20)
 emp_id int primary key,
 salary int
```

The available types are:

```
char(len)
int
real
```

**C.2.2 The Drop Clause.** The Drop Clause is used to remove a table definition from the database:

```
DROP TABLE table_name
```

For example:

```
DROP TABLE emp_details
```

**C.2.3 The Insert Clause.** Unlike ANSI SQL, the user cannot nest a Select within an Insert (i.e., the user cannot insert the data returned by a select). Currently, the user must also specify the names of the fields into which the data is to be inserted. The user cannot specify the values without the field name and expect the server to insert the data into the correct fields by default.

```
DELETE FROM table_name
WHERE column OPERATOR value
[AND | OR column OPERATOR value]**
OPERATOR can be <, >, =, <=, >=, <>, or like
```

For example:

```
DELETE FROM emp_details WHERE emp_id = 12345
```

The number of values supplied must match the number of columns.

**C.2.4 The Select Clause.** The Select Clause offered by mSQL lacks some of the features provided by the SQL specification:

- No nested selects
- No implicit functions (e.g., count(), avg() ).

It does, however, support:

- Joins
- DISTINCT row selection
- ORDER BY clauses
- Regular expression matching
- Column-to-column comparisons in WHERE clauses.

The formal syntax for mSQL's select is:

```
SELECT [table.]column [, [table.]column]**
FROM table[, table]**
[WHERE [table.]column OPERATOR VALUE
[AND | OR [table.]column OPERATOR VALUE]**]
[ORDER BY [table.]column[DESC][, [table.]column[DESC]]
OPERATOR can be <, >, =, <=, >=, <>, or like
VALUE can be a literal value or a column name
```

A simple select may be:

```
SELECT first_name, last_name FROM emp_details
```

```
WHERE dept='finance'
```

To sort the returned data in ascending order by last\_name, and descending order by first\_name, the query would look like this:

```
SELECT first_name, last_name FROM emp_details
WHERE dept='finance'
ORDER BY last_name, first_name DESC
```

And to remove any duplicate rows, the DISTINCT operator could be used:

```
SELECT DISTINCT first_name, last_name FROM emp_details
WHERE dept='finance'
ORDER BY last_name, first_name DESC
```

The regular expression syntax supported by LIKE clauses is that of standard SQL:

- '\_' matches any single character
- '%' matches ) or more characters of any value
- '\\' escapes special characters (e.g. '\\%' matches % and '\\\\' matches \\ )
- all other characters match themselves.

For example, to search for anyone in Finance whose last name consists of a letter followed by 'ughes', such as Hughes, the query could look like this:

```
SELECT first_name, last_name FROM emp_details
WHERE dept='finance' and last_name like '_ughes'
```

The power of a relational query language becomes apparent when the user starts joining tables together during a select. For example, consider a task where a user has two tables defined, one containing staff details and another listing the projects being worked on by each staff member, and each staff member has been assigned a unique employee number. The user could generate a sorted list of who was working on what project with a query such as this:

```
SELECT emp_details.first_name, emp_details.last_name,
project_details.project
FROM emp_details, project_details
WHERE emp_details.emp_id=project_details.emp_id
ORDER BY emp_details.last_name, emp_details.first_name
```

mSQL places no restriction on the number of tables "joined" during a query; therefore if there are 15 tables containing information related to an employee ID in some manner, data from each of those tables could be extracted (albeit slowly), by a single query. One key point to note regarding joins is that the user must qualify all column names with a table name. mSQL does not support the concept of uniquely named columns spanning multiple tables, so the user is forced to qualify every column name if accessing more than one table in a single select.

**C.2.5 The Update Clause.** The mSQL Update clause cannot use a column name as a value. Only literal values may be used as an update value.

```
UPDATE table_name SET column=value[,column=value]**
WHERE column OPERATOR value
[AND | OR column OPERATOR value]**
OPERATOR can be <, >, =, <=, >=, <>, or like
```

For example:

```
UPDATE emp_details SET salary=30000 WHERE emp_id=1234
```

### C.3 The mSQL Terminal Monitor

Like all database applications, mSQL provides a program that allows a user to interactively submit queries to the database engine. In mSQL, it is a program simply called 'msql'. It requires one command line argument, which is the name of the database to access. Once started, there is no way to swap databases without restarting the program.

The monitor also accepts two command line flags:

- -h *Host* Connect to the mSQL server on *Host*.
- -q Process one query and quit returning an exit code.

The monitor has been modelled after the original Ingres (and the subsequent Postgres) monitor program. Commands are distinguished from queries by backslash prefixes. To obtain help from the monitor prompt, the \h command is used. To exit from the program, the \q command or an EOF(^D) must be entered.

To send a query to the engine, the query is entered followed by the \g command. \g tells the monitor to "Go" and send the query to the engine. If the user wishes to edit the last query, \e will place the user inside of the vi editor, where the query can be modified. If the user wishes to use an editor other than the vi editor to perform query editing, mSQL will honor the convention of using the contents of the VISUAL environment variable as an alternate editor. When the user has completed the editing, exiting the editor in the usual manner will return the user to mSQL with the edited query placed in the buffer. The query can then be submitted to the server by using the \g "Go" command as usual.

The query buffer is maintained between queries not only to enable query editing, but also to allow a query to be submitted multiple times. If \g is entered without entering a new query, the last query to be submitted will be resubmitted. The contents of the query buffer can also be displayed by using the \p "Print" command of the monitor.

To enable convenient access to database servers running on remote hosts, the mSQL terminal monitor supports the use of an environment variable to indicate the machine running the server (rather than having to specify -h *some.hosts.name* every time the user executes mSQL). Note that this



is a function provided by the mSQL terminal monitor, not the mSQL API library, and as such is not available for use with other programs. To use this feature, set the environment variable `MSQL_HOST` to the name or address of the desired machine.

#### C.4 mSQL Database Administration

mSQL databases are administered using the *msqladmin* command. Several administrative tasks, such as creating new databases and forcing a server shutdown, are performed using *msqladmin*. Like all mSQL programs, *msqladmin* accepts the `'-h Host'` command line flag to specify the desired machine. The commands available via *msqladmin* are:

- `create DataBase` Create a new database called *DataBase*
- `drop DataBase` Delete the entire database called *DataBase*
- `shutdown` Tell the server to shut itself down
- `reload` Tell the server to reload its access control information
- `version` Display various version information from the server.

It should be noted that the server will only accept *create*, *drop*, *shutdown*, and *reload* commands if they are sent by the root user (as defined at installation time) and are sent from the machine running the server. An attempt to perform any of these commands from a remote client or as a non-root user will result in a "permission denied" error. The only command a user can execute over the network or as a non-root user is *version*.

#### C.5 mSQL Schema Viewer

mSQL provides the *relshow* command to display the structure of a database. If executed with no arguments, *relshow* will list the available database. If it is executed with the name of a database, *relshow* will list the tables that have been defined for that database. If given both a database and table name, *relshow* will display the structure of the table including the field names, types, and sizes. Like all mSQL programs, *relshow* honors the `'-h Host'` command line flag to specify a remote machine as the database server.

#### C.6 mSQL Database Dumper

A program is provided that will dump the contents and structure of a table or entire database in an ASCII form. The program, *msqldump*, produces output that is suitable to be read by mSQL terminal monitor as a script file. Using this tool, the contents of a database can be backed-up or moved to a new database. By virtue of the `'-h Host'` option, the contents of a remote database may be pulled in over the net. This can be used as a mechanism for mirroring the contents of an mSQL database onto multiple machines.

## C.7 Access Control

Access control is managed by the *mysql.acl* file in the installation directory. This file is split into entries for each database to be controlled. If the file doesn't exist or details for a particular database aren't configured, access reverts to global read/write. This is an example of an acl entry:

```
Sample access control for mSQL
database=test
read=bambi,paulp
write=root
host=*.Bond.edu.au,student.it.Bond.edu.au
access=local,remote
```

Using this definition, database 'test' can be accessed by both local and remote connections from any host in the *Bond.edu.au* domain except for the *student.it.Bond.edu.au*. Read access is only granted to *bambi* and *paulp*. Nobody else is allowed to perform selects on the database. Write access is only available to *root*.

Control is based on the first match found for a given item. Thus, a line such as "read=\*,bambi" would not get the desired results (i.e., deny access to everyone other than bambi) because *\** will also match bambi. In this case, the line would have to be "read=bambi,\*" although the *\** is superfluous as that is the default action.

Note that if an entry isn't found for a particular configuration line (such as "read") it defaults to a global denial. For example, if there is no "read" line (i.e., there are no "read" tokens after the data is loaded) nobody will be granted "read" access. This is in contrast to the action taken if the entire database definition is missing, in which case access to everything is granted.

Another feature to note is that a database's entry must be followed by a blank line to signify the end of the entry. There may also be multiple config lines in the one entry (such as "read=bambi,paulp" "read=root"). The data will be loaded as though it was concatenated onto the same "read" line (i.e., "read=bambi,paulp,root").

Wild cards can be used in any configuration entry. A wild card by itself will match anything whereas a wild card followed by some text will cause only a partial wild card (e.g., *\*.Bond.edu.au* matches anything that ends in *Bond.edu.au*). A wild card can also be set for the database name. A good practice is to install an entry with *database=\** as the last entry in the file so that if the database being accessed wasn't covered by any of the other rules a default site policy can be enforced.

The acl information can be loaded at runtime using *mysqladmin reload*. This will parse the file before it sends the reload command to the engine. Only if the file is parsed cleanly is it reloaded. Like most *mysqladmin* commands, it will only be accepted if generated by the root

user (or whoever the database was installed as) on the local host.

### C.8 Drop\_buttons

The *drop\_buttons* script located in */h/EM/progs* allows the user to list which buttons are stored in the mysql gccs database, and to drop buttons if the associated application has been de-installed from all platforms at the site.

The following command will list all buttons stored in the mysql gccs database:

```
/h/EM/progs/drop_buttons -l
```

To look for a specific button or group of buttons, enter the following command:

```
/h/EM/progs/drop_buttons -l {Actual name of button or first few
characters}
```

To drop a button, enter the following:

```
/h/EM/progs/drop_buttons -l {Actual name of button}
```

The program will ask for confirmation that the user wishes to drop the specified button.

## APPENDIX D. SITE DOMAIN NAMES

Site domain names and related DNS procedures are provided in the following message:

DISA ADEPT #260 & DTG 191752Z OCT 95..

FM DISA WASHINGTON DC//D23//  
TO CNO WASHINGTON DC//N62//  
PM AWIS FT BELVIER VA//SFAE-CC-AWT//  
HQ USAF WASHINGTON DC//SCMC//  
DISA WASHINGTON DC//D6/D2/D23/JEJIT/JEAB/JEEFE/WE163/WE225//  
COMMARCONSYSCON QUANTICO VA//C41DPR//  
CMC WASH DC//POC-30//  
SSG MAXWELL AFB GUNTER ANNEX AL//SIF/SSG/SIN//  
AIG 8787  
AIG 8791  
SAF WASHINGTON DC//AQPC//  
HQ ESC HANSCOM AFB MA//AVN//  
HQ AFC4A SCOTT AFB IL//XPR//  
COMSPAWARSSYSCOM WASHINGTON DC//PMW171//  
JCS WASHINGTON DC//J6V//  
COMNAVCOMTELCOM WASHINGTON DC//N2//  
NCTAMSLANT NORFOLK VA//N2//  
NAVCOMTELSTA PENSACOLA FL//N3//  
MCTSSA EAST QUANTICO VA//DIR/NOC//  
CMC WASHINGTON DC//PPO/C4I/AR//  
CG MCCDC QUANTICO VA//AS//  
COMMARCONSYSCOM QUANTICO VA//C4I/CIS//  
MCTSSA CAMP PENDLETON CA//JJJ//  
CDR USAISC FT HUACHUCA AZ//ASOP-OP//  
BT  
UNCLAS

SUBJ: CONSOLIDATION OF DOMAIN NAME SERVICE (DNS) FOR THE GLOBAL COMMAND AND CONTROL SYSTEM (GCCS) (U)

1. THE SIPRNET SUPPORT CENTER (SSC) IS OPERATIONAL. PHONE NUMBERS ARE (800)-582-2567 OR (703) 802-8202. THE SSC IS THE SECRET LEVEL, CLASSIFIED EQUIVALENT OF THE MILNET/NIPRNET NETWORK INFORMATION CENTER (NIC). THE SSC IS RESPONSIBLE FOR ALL SIPRNET VALUE ADDED SERVICES FOR THE SECRET DOD COMMUNITY.

2. CONSOLIDATION OF THE GCCS DNS SERVICE WITH THE STANDARD SSC DNS SERVICE REQUIRES CLOSE COORDINATION WITH THE SSC. THE FOLLOWING DIRECTIVE AND INFORMATION ADVISORY IS PROVIDED TO GCCS SITES.

3. DIRECTIVE: ALL SITES IMPLEMENTING GCCS SHALL IMPLEMENT DNS AS THE UNIQUE NETWORK DEVICE NAMING SERVICE.

A. ALL NEW REQUESTS FOR IP NETWORK NUMBERS (CLASS B OR C), DOMAIN NAMES, AUTONOMOUS SYSTEM NUMBERS, ETC. SHALL BE DIRECTED TO THE SSC, EFFECTIVE IMMEDIATELY.

B. THE ".MIL" DOMAIN IDENTIFIER SHALL BE ADDED TO EACH ".SMIL" IDENTIFIER. THE ROOT DOMAIN IDENTIFIER FOR ALL SECRET DOD USERS IS ".SMIL.MIL".

C. IN COMPLYING WITH THE NAMING STANDARDS, THE ".GCC.SMIL" DOMAIN WILL BE ABANDONED. EACH ".GCC" SITE WILL BE CONVERTED TO THE APPROPRIATE SERVICE/AGENCY (S/A) OR COMMAND NAME SIMILAR TO CURRENT MILNET REGISTRATION ON THE UNCLASSIFIED MILNET. THE FOLLOWING IDENTIFIES ESTABLISHED DNS SERVERS UNDER THE ".GCC.SMIL" DOMAIN. THEY MUST BE CHANGED TO THE NEW SIPRNET COMPLIANT NAMING STRUCTURE IDENTIFIED BELOW. THE SIPRNET COMPLIANT NAME HAS BEEN COORDINATED WITH THE SSC AND THE S/A DOMAIN MANAGERS TO ENSURE THE DOMAIN NAMING SCHEME IS CORRECT.

| GCCS SITE   | GCC DNS NAME          | SIPRNET DNS NAME           |
|-------------|-----------------------|----------------------------|
| ACC         | .ACC.GCC.SMIL         | .ACC.LANGLEY.AF.SMIL.MIL   |
| ACOM        | .ACOM.GCC.SMIL        | .ACOM.SMIL.MIL             |
| AFMC        | .AFMC.GCC.SMIL        | .AFMC.WPAFB.AF.SMIL.MIL    |
| AMC         | .AMC.GCC.SMIL         | .AMC.SCOTT.AF.SMIL.MIL     |
| AREUR       | .AREUR.GCC.SMIL       | .AREUR.ARMY.SMIL.MIL       |
| ARPAC       | .ARPAC.GCC.SMIL       | .ARPAC.ARMY.SMIL.MIL       |
|             |                       | .ARSOC.ARMY.SMIL.MIL       |
|             |                       | .ARSOC.SMIL.MIL **         |
| CENTAF      | .CENTAF.GCC.SMIL      | .CENTAF.SHAW.AF.SMIL.MIL   |
| CENTCOM     | .CENT.GCC.SMIL        | .CENTCOM.SMIL.MIL          |
| CINCLANTFLT | .CINCLANT.GCC.SMIL    | .CINCLANT.NAVY.SMIL.MIL    |
| CNO         | .CNO.GCC.SMIL         | .CNO.NAVY.SMIL.MIL         |
| DISA-JDEF   | .JDEF.GCC.SMIL        | .JDEF.DISA.SMIL.MIL        |
| DISA-JITC   | .JITC.GCC.SMIL        | .JITC.DISA.SMIL.MIL        |
| DISA-OSF    | .OSF.GCC.SMIL         | .OSF.DISA.SMIL.MIL         |
| EUCOM       |                       | .EUCOM.SMIL.MIL            |
| FORSCOM     | .FORCE1.GCC.SMIL      | .FORSCOM.ARMY.SMIL.MIL     |
|             |                       | .FORCE1.SMIL.MIL           |
| HQAF        | .HQAF.GCC.SMIL        | .HQAF.PENTAGON.AF.SMIL.MIL |
| HQDA        | .HQDA.GCC.SMIL        | .HQDA.ARMY.SMIL.MIL        |
|             | .AOC.GCC.SMIL         | .AOC.ARMY.SMIL.MIL         |
| HQMC        | .HQMC.GCC.SMIL        | .HQMC.USMC.SMIL.MIL        |
| JTO         | .JTO.GCC.SMIL         | .JTO.SCOTT.AF.SMIL.MIL     |
| MARFORCENT  |                       | .MFC.USMC.SMIL.MIL         |
| MARFOREUR   |                       | .MFE.USMC.SMIL.MIL         |
| MARFORLANT  | .MARFORLANT.GCC.SMIL  | .MFL.USMC.SMIL.MIL         |
| MARFORPAC   | .MFP.GCC.SMIL         | .MFP.USMC.SMIL.MIL         |
| MSC         | .MSC.GCC.SMIL         | .MSC.NAVY.SMIL.MIL         |
| MTMC        | .MTMC.GCC.SMIL        | .MTMC.ARMY.SMIL.MIL        |
| NAVCENT-R   | .DEP-NAVCENT.GCC.SMIL | .NAVCENT-R.NAVY.SMIL.MIL   |
| NAVCENT-F   | .NAVCENT.GCC.SMIL     | .NAVCENT-F.NAVY.SMIL.MIL   |
| NAVEUR      | .NAVEUR.GCC.SMIL      | .NAVEUR.NAVY.SMIL.MIL      |
| NAVSOC      | .NAVSOC.GCC.SMIL      | .NAVSOC.NAVY.SMIL.MIL      |
| NMCC        | .NMCC.GCC.SMIL        | .NMCC.SMIL.MIL             |
| NMCC-R      | .ANMCC.GCC.SMIL       | .NMCC-R.SMIL.MIL           |
| PACAF       | .PACAF.GCC.SMIL       | .PACAF.HICKAM.AF.SMIL.MIL  |
| PACFLT      | .PACFLT.GCC.SMIL      | .PACFLT.NAVY.SMIL.MIL      |
| PACOM       | .PACOM.GCC.SMIL       | .PACOM.SMIL.MIL            |
|             |                       | .PACOM.GCC.SMIL.MIL**      |
| SOCOM       | .SOCOM.GCC.SMIL       | .SOCOM.SMIL.MIL            |

|          |                    |                              |
|----------|--------------------|------------------------------|
| SOUTHCOM |                    | .SOUTHCOM.SMIL.MIL           |
| SPACECOM | .SPACECOM.GCC.SMIL | .SPACECOM.SMIL.MIL           |
| STRATCOM | .STATCOM.GCC.SMIL  | .STRATCOM.OFFUTT.AF.SMIL.MIL |
| TRANSCOM | .USTC.GCC.SMIL     | .USTC.SMIL.MIL               |
| USAFE    | .USAFE.GCC.SMIL    | .USAFE.RAMSTEIN.AF.SMIL.MIL  |
| USFK-T   | .USFK.GCC.SMIL     | .USFK-T.ARMY.SMIL.MIL        |
| USFK-Y   | .USFK.GCC.SMIL     | .USFK-Y.ARMY.SMIL.MIL        |

\*\* CURRENT DOMAIN INCORRECTLY REGISTERED WITH SSC. INCORRECTLY REGISTERED DOMAINS WILL BE DELETED WHEN THE APPROPRIATE DOMAIN ADMINISTRATOR NOTIFIES THE SSC.

D. IN COMPLYING WITH THE NAMING STANDARDS AND TO ENSURE INTEROPERABILITY, THE OLD SET OF LOCAL ".SMIL" AND ".GCC.SMIL" DOMAIN AND SERVER NAMES WILL BE IDENTIFIED "ALIASED" AS AUXILIARY DNS NAME SETS ON LOCAL NAME SERVER DNS FILES UNTIL ALL SITES HAVE BEEN MIGRATED AND APPLICATIONS REFLECT THE REVISED NAMES. THESE ALIASED NAME SETS WILL ENSURE CONTINUED COMMUNICATIONS WITHIN THE GCCS COMMUNITY. THESE ORIGINAL NAMES SETS WILL BE DELETED 60 DAYS AFTER THE DTG OF THIS MESSAGE. TECHNICAL INFORMATION WILL BE AVAILABLE TO WEB BROWSERS AT URL=FTP://HORNET.OSF.GCC.SMIL/PUB/DNS (EXISTING) AND URL=FTP://HORNET.OSF.DISA.SMIL.MIL/PUB/DNS (PENDING).

E. THESE CHANGES WILL BE MADE SITE BY SITE IN COORDINATION WITH THE SSC, THE S/A DOMAIN MANAGERS, AND THE .GCC DOMAIN ADMINISTRATOR. EACH SITE MUST CONTACT THE SSC BY COB 23OCT95 TO DISCUSS THE MIGRATION FOR BOTH .SMIL.MIL AND .GCC.SMIL.MIL CONVERSIONS. FOURTH LEVEL DOMAINS AND BELOW, E.G., USAFE.RAMSTEIN.AF.SMIL.MIL NEED NOT COORDINATE WITH THE SSC BUT THEY MUST COORDINATE WITH THE S/A DOMAIN MANAGER. ALL THIRD LEVEL DOMAINS MUST COORDINATE WITH THE SSC. IT IS HIGHLY RECOMMENDED THAT ALL FOURTH LEVEL AND LOWER DOMAINS REGISTER WITH THE SSC. THIS REGISTRATION IS FOR DIRECTORY INFORMATION ONLY AND IS NOT REQUIRED FOR DNS. ALL THIRD LEVEL DOMAINS MUST REGISTER WITH THE SSC AND MUST BE APPROVED BY THE DISA SSC MANAGER.

F. SITES MUST NOT MAKE ANY DNS CHANGES PRIOR TO CONSULTING WITH THE S/A DOMAIN MANAGERS AND THE SSC.

G. THE FOLLOWING S/A SUBDOMAINS TO THE SIPRNET ".SMIL.MIL" DOMAIN MUST BE ESTABLISHED AND IN PLACE TO AID THE GCCS COMMUNITY IN COMPLYING WITH THE NAMING STANDARDS.

|      |                |                                      |
|------|----------------|--------------------------------------|
| AF   | .AF.SMIL.MIL   | ACTIVATED                            |
| ARMY | .ARMY.SMIL.MIL | ACTIVATION PENDING, ESTIMATED 951025 |
| NAVY | .NAVY.SMIL.MIL | ACTIVATED                            |
| USMC | .USMC.SMIL.MIL | ACTIVATED                            |
| DISA | .DISA.SMIL.MIL | ACTIVATION PENDING, ESTIMATED 951020 |

#### 4. ADVISORY:

A. 'WHOIS' CAPABILITY ACCESS IS THROUGH THE SIPRNET WEB SERVER AT SSC.SMIL.MIL OR IP ADDRESS 204.34.130.5. WHOIS IS ALSO AVAILABLE VIA TELNET TO SSC.SMIL.MIL OR IP ADDRESS 204.34.130.5. AFTER OPENING THE TELNET CONNECTION TYPE WHOIS TO BEGIN SESSION. THE WHOIS IS ALSO

AVAILABLE VIA EMAIL TO SERVICE@SSC.SMIL.MIL. PLACE WHOIS XXX (WHERE XXX IS THE QUERY DESIRED) IN THE SUBJECT LINE OF THE MESSAGE. THE RESULTS OF THE QUERY WILL BE RETURNED VIA EMAIL.

B. THE SIPRNET WEB SERVER IS ACCESSIBLE AT HTTP://SSC.SMIL.MIL OR HTTP://204.34.130.5. USE THE MOSAIC OR THE NETSCAPE WEB BROWSER APPLICATION INSTALLED ON THE GCCS WORKSTATIONS TO ACCESS THE WEB SITE.

C. TO POPULATE THE SSC DATA BASES FOR DIRECTORY SERVICES, SITES MUST BEGIN IMMEDIATELY TO REGISTER INSTALLED DOMAIN NAME SERVERS (AFTER CONVERSIONS), EMAIL USERS, POC'S FOR SITES AND HOST ADMINISTRATORS, IP ADDRESSES, DOMAIN NAMES, AND AUTONOMOUS SYSTEM NUMBERS WITH THE SSC. REGISTRATION INFORMATION AND TEMPLATES ARE AVAILABLE THROUGH THE SSC WEB SERVER. TEMPLATES ARE ALSO AVAILABLE THROUGH ANONYMOUS FTP TO SSC.SMIL.MIL. CHANGE TO THE TEMPLATES DIRECTORY AND GET THE APPROPRIATE TEMPLATE FILE. TEMPLATES ARE ALSO AVAILABLE THROUGH EMAIL. EMAIL TO SERVICE@SSC.SMIL.MIL. PUT TEMPLATE/<FILENAME> IN THE SUBJECT LINE. TEMPLATE WILL BE RETURNED VIA EMAIL. HOST REGISTRATIONS FOR ALL HOSTS THAT ARE MEMBERS OF THIRD LEVEL AND BELOW DOMAINS MUST PASS THROUGH THE APPROPRIATE DOMAIN ADMINISTRATOR PRIOR TO BEING SENT TO THE SSC. THIS WILL ENSURE THAT THE APPROPRIATE DOMAIN ADMINISTRATOR IS AWARE OF THE HOST AND ADDS IT TO THEIR ZONE FILE. THIS WILL ALSO ENSURE THAT HOSTS THAT ARE MEMBERS OF NETWORKS THAT DO NOT HAVE INADDR SERVERS WILL BE INCLUDED IN THE TOP LEVEL INADDR.ARPA ZONE SO THAT REVERSE MAPPING WILL WORK. WHERE POSSIBLE ALL NETWORKS SHOULD ESTABLISH INADDR SERVERS TO THAT THE NETWORK INADDR CAN BE DELEGATED FROM THE TOP LEVEL INADDR.ARPA ZONE.

D. TO PERMIT TIMELY SSC AND GCCS INFORMATION TO BE E-MAILED TO SITES, ALL DOMAIN ADMINISTRATORS SHALL IMMEDIATELY ESTABLISH THE E-MAIL ALIAS "POSTMASTER@<DOMAIN>.SMIL.MIL" OR "POSTMASTER@>DOMAIN.SMIL" (REFERENCE DDN MGT BULLETIN: 9507) ON THE SITE'S PRINCIPAL SIPRNET MAIL RELAY, WHERE <DOMAIN> IS THE SITE'S REGISTERED DOMAIN NAME. THIS ALIAS SHALL RESOLVE TO A RESPONSIBLE TECHNICAL STAFF ELEMENT.

E. FUTURE GCCS SITES REQUIRING SIPRNET COMPLIANT DNS ARE: 3WG, 5AF, 7AF, 8AF, 11AF, 13AF, 18WG, 36AW, 51FW, 354FW, 374AW, 613ACOMS, 20AF, AETC, AFMPC, AFRES, AFSOC, AFSPACE, AFWC, ALOM, AOC, ARCENT, ARSPACE, AWC, COMICEDEFOR, COMUSFORAZ, COMUSJAPAN, DISA-EUR, DISA-PAC, JSOC, MARFORCENT, MARFOREUR, NAVSPACE, NAVSPECWAR, NORAD, NPS, NSA, NWC, SOCPAC, SOCSOUTH, USARJ, USARSO, AND USASOC.

F. IT MAY BE NECESSARY FOR SOME GCCS LOCATIONS TO TEMPORARILY SUPPORT MULTIPLE DOMAINS WHILE THE SECRET LEVEL DNS STRUCTURE IS ESTABLISHED WITHIN THE DOD COMMUNITY. FOR EXAMPLE, ACC IS RESPONSIBLE FOR THE .ACC.LANGLEY.AF.SMIL.MIL DOMAIN. HOWEVER, THEY MAY NEED TO TEMPORARILY SUPPORT THE .LANGLEY.AF.SMIL.MIL DOMAIN UNTIL SUCH TIME THE LANGLEY DOMAIN MANAGER CAN ASSUME CONTROL. ALL DOMAINS BELOW THE THIRD LEVEL MUST BE COORDINATED WITH THE S/A DOMAIN MANAGER.

G. S/A DOMAIN MANAGERS ARE:

|      |               |             |                                     |
|------|---------------|-------------|-------------------------------------|
| AF   | MR. HOSTETTER | DSN596-3126 | AFDOMAIN@SERVER.AF.MIL              |
| ARMY | MR. TRADER    | DSN879-7250 | TRADERW@HAUCHUCA-<br>EMH12.ARMY.MIL |
| NAVY | MR. GREUNKE   | DSN992-3501 | STEVE.GREUNKE@NCTS.NAVY.MIL         |
| USMC | CAPT GONTER   | DSN278-5988 | GONTERT@MQG-SMTP3.USMC.MIL          |

DISA AND GCCS  
MR. LEE DSN653-8631    LEEM@NCR.DISA.MIL  
                          MLEE@OSF.GCC.SMIL (CURRENT)

5. POINTS OF CONTACT

A. MARY JANE HALEY, DISA//JIEO/JEJIT/, (703)-735-8542, DSN 653-8542, SIPRNET E-MAIL HALEYM@HORNET.OSF.GCC.SMIL.MIL, UNCLASS E-MAIL HALEYM@NCR.DISA.MIL.

B. MARVIE LEE, DISA//JIEO/JEJI//, (703) 735-8631, DSN 653-8631, SIPRNET E-MAIL MLEE@HORNET.OSF.GCC.SMIL.MIL, HOSTMASTER@OSF.GCC.SMIL, UNCLASS E-MAIL LEEM@NCR.DISA.MIL.

C. CAPT GREG CSEHOSKI, DISA//JEAB//, (703)-735-8760, OR DSN 653-8760, UNCLASS E-MAIL CSEHOSKG@NCR.DISA.MIL.

D. SIPRNET SUPPORT CENTER (SSC), HELP DESK: 7 A.M. - 7 P.M. EASTERN TIME 1 (800) 582-2567 - CONUS ONLY, (703) 802-8202, E-MAIL: HOSTMASTER@SSC.SMIL.MIL, REGISTRAR@SSC.SMIL.MIL, SSC@SSC.SMIL.MIL, HOMEPAGE: HTTP://SSC.SMIL.MIL, FTP: SSC.SMIL.MIL, TELNET: SSC.SMIL.MIL

6. THIS MESSAGE HAS BEEN COORDINATED WITH AND APPROVED BY THE JOINT STAFF//J3/J4/J6, DISA/WESTHEM/WE3353, AND THE S/A DOMAIN MANAGERS.//  
BT



## APPENDIX E. ESTABLISHING THE ACCOUNT FOR USER *news*

The Internet News Server is a daemon. For correct operation, it executes as user *news* and group *mail*. Solaris is shipped with an entry in */etc/passwd* for the user *news*. However, the home directory for *news* is set to */var/spool/news*; this directory is not created when Solaris is installed. To ensure correct operation of the News Server, create this directory using the following commands:

```
mkdir -p /var/spool/news
chown news /var/spool/news
chgrp mail /var/spool/news
```

---

**NOTE:** It does not matter if the News Server has already been installed; these commands can be executed before or after segment installation.

---

HP-UX does not have a user *news* in the password file (*/etc/passwd*) when installed, and the Internet News Server Segment does not create an account for this user. Thus, prior to installing the Internet News Server, you must create an account for *news*. This user should have the user ID "6", login name "news", and the primary group "mail" (group ID "6"). Set the encrypted password for *news* in */etc/passwd* to "\*", which prevents users from logging into this account.

## **APPENDIX F.     SYSTEM BACKUP AND RECOVERY**

### **F.1     Scope**

The section addresses the backup of all critical data in the GCCS system. It also covers the recovery procedures in the event of the loss of a system or the corruption of critical data. It does not address the backup and recovery of Oracle, which is covered in another section.

### **F.2     System Backup Strategy**

It is recommended, if resources permit, that a backup Executive Manager (EM) server be identified at a site. This would facilitate the rapid activation of the backup EM server should the primary EM server fail. This platform should have the Sybase partitions defined and have the Sybase segment installed, but not initialized.

The *System Backup* segment, described below, saves all the information required to recover from a system hardware or software failure. It should be installed on all GCCS platforms. In addition to the backups performed by the *System Backup* segment, it is highly recommended that a level-zero dump be performed on each platform after it has been built. This will enable you to rapidly recover if you lose a disk drive.

### **F.3     System Backup Segment Description**

A segment called *System Backup* has been developed to automatically back up all data needed to rebuild or recover from the failure of a key server, e.g. the NIS+, DNS, Sybase, and particularly the EM server. During installation the *System Backup* segment creates a crontab entry to launch the *system\_backup* at the time identified by the installer. Crontab entries to dump the NIS+ passwords and the Sybase logs are also created on the appropriate servers. During execution, the *System Backup* segment will automatically determine if the platform on which it is running is the NIS+, Sybase, EM, and/or DNS server. Based on this determination it backs up the appropriate data as listed below. In addition to the data mentioned below, a report on all segments/SUN OS patches installed on a system will be generated daily in */h/USERS/BACKUP/local*. Any files and/or directories identified by links in */h/data/local/backup* will also be backed up in */h/USERS/BACKUP/local*. Finally, as part of the backup process the systems will be cleaned up through the removal of all core files, old EM log files, and extraneous data in */tmp* and */var/tmp*.

The *System Backup* segment should be installed on all systems. At the very least it will create a daily report of what is installed on each platform. Since it automatically determines what should be backed up, it will always save the data needed to recover if the NIS+, Sybase, the EM, or DNS server goes down.

Backups will occur on a daily basis, at a time specified by the installer when this segment is installed for the first time at a site. If no time is specified, 2200 hours will be used as a default. All

backed up data is stored in */h/USERS/BACKUP*. The *System Backup* segment will also create a root crontab job to tar */h/USERS* to tape on a daily basis, if the installer provides a system name when asked. The time can also be specified by the installer. If none is specified, the tar will occur one hour after the backup time, or 2300 hours by default. If no tape or tape drive is available when the tar cron job is scheduled, all data will be archived for a maximum of three days and a message explaining this will be sent to the Security Manager (secman).

An icon has also been provided to the System Administrator (sysadmin) that will allow the System Administrator to back up the system at any time. If executed on the server designated for doing the tape backups of */h/USERS*, it will execute the tape backup. In addition, an icon has been provided that allows the System Administrator to change the system backup time, the tape backup time, the tape backup platform, and/or tape drive. Changes to the system backup time become effective when *system\_backup* executes at the original time. Changes to the remaining parameters become effective immediately.

#### **F.4 Specific Data Backed Up**

##### **F.4.1 NIS+ Server**

On the NIS+ server a checkpoint of the NIS+ logs is executed and then a *nisaddent* is executed on the hosts, passwd, group, and shadow tables at the specified time. The resulting hosts, passwd, group, shadow files are stored in */etc/nis*. The last two days of these files are always available in */etc/nis*. A *nisaddent* is executed on the shadow file every hour to ensure that any user changes of their password are captured. The last three hours of the shadow files are always maintained in */etc/nis*.

At the specified time a compressed tar file called *NIS.tar.Z* is created in */h/USERS/BACKUP*. This file contains the following files and directories: */etc/nis*, */etc/.rootkey*, */etc/defaultdomain*, */etc/nsswitch.conf*, and */var/nis*.

##### **F.4.2 Sybase Server**

On the Sybase server, the GCCS database is dumped at the specified time into */h/USERS/BACKUP/sybase*. This database contains all user data stored in folders. The transaction logs for the GCCS database are dumped at 6:00, 10:00, 14:00, 18:00, and 22:00 hours.

##### **F.4.3 Executive Manager Server**

On the EM server, a compressed tar file called *GLOBAL.tar.Z* will be created in */h/USERS/BACKUP*. This file will contain the entire contents of */h/data/global*. A compressed tar file called *MSQL.tar.Z* will also be created in */h/USERS/BACKUP*. This file will contain the msql database (*/h/data/global/EMDATA/msql*), which contains all user profile information and data on all desktop icons.

#### F.4.4 DNS Server

On the DNS server, a compressed tar file called *DNS.tar.Z* is stored in */h/USERS/BACKUP* at the specified time. The contents of this file are the file */etc/name.boot* and the directory */var/nameserver*.

#### F.4.5 All GCCS Systems

A mechanism has been developed to enable applications to identify data that should be backed up. A directory called *backup* is created in */h/data/local* by the *System Backup* segment. Any application having data that should be backed up should place a link in */h/data/local/backup* that points to the data. A root crontab entry is created on all systems on which the *System Backup* segment is installed; it backs up all linked data at the specified time. This crontab entry also creates a daily report of what segments and Solaris patches are installed on the system. These reports and the data identified in */h/data/local/backup* are stored in */h/USERS/BACKUP/local*. Finally, system cleanup is also executed to remove old core files, log files, and clean out */tmp*.

### F.5 Recovery

**F.5.1 NIS+.** If the NIS+ database becomes corrupted, or the NIS+ server goes down, the data backed up in */h/USERS/BACKUP/NIS.tar.Z* or in */etc/nis* will have to be used to recover. In the case of a corrupted NIS+ database you may be able to simply replace the NIS+ tables in */var/nis* to recover (see F.5.1.1). In the case where the NIS+ server goes down, or the procedures in paragraph F.5.1.1 did not correct the problem, you will have to rebuild the NIS+ server (F.5.1.2).

#### F.5.1.1 NIS+ Database Corrupted Recovery Procedures

- a. On the original NIS+ server, execute the following to kill the NIS+ processes:

```
/etc/nis/admin/nis_kill<return>
init 6<return>
```

- b. Execute the following to protect files currently stored in */etc/nis*:

```
mv /etc/nis /etc/nis_save <return>
```

- c. The files contained in *NIS.tar.Z* are in absolute tar format. Consequently, they will be automatically placed in the correct location when they are extracted. Execute the following to extract the NIS+ tables:

```
zcat /h/USERS/BACKUP/NIS.tar.Z | tar xvf - <return>
```

- d. Reboot the system to restart NIS+ by executing the following:

```
uadmin 2 1 <return>
```

- e. View the database to verify that NIS+ is running properly by executing the following:

1. List all tables in NIS+

```
nislsl org_dir <return>
```

2. List cache information:

```
nisshowcache <return>
```

3. List user accounts:

```
niscat passwd.org_dir <return>
```

- f. Reboot all client platforms to re-initialize NIS+ on them.

#### **F.5.1.2 NIS+ Server Rebuilding Procedures**

- a. On the NIS+ server execute the following to kill NIS+ processes:

```
/etc/nis/admin/nis_kill<return>
init 6<return>
```

- b. If you are on the original NIS+ server and the group, passwd, shadow, and hosts files in /etc/nis are correct, skip this step; otherwise execute the following:

```
zcat /h/USERS/BACKUP/NIS.tar.Z | tar xvf - /etc/nis
<return>
```

- c. In preparation for setting up the NIS+ server execute the following:

```
cd /etc/nis <return>
chgrp 101 * <return>
chmod 664 * <return>
sh <return>
PATH=$PATH:/usr/lib/nis; export PATH <return>
```

- d. Create the NIS+ server by executing the following:

```
nisserver -r -d {Enter the NIS+ DOMAINNAME}. <return>
```

This script sets up this machine "rootmaster" as a NIS+ Root master Server for the domain {NIS DOMAINNAME}. The following will be displayed on the screen:

```
Domainname : {NIS DOMAINNAME}
```

```
NIS+ Group : admin.{NIS DOMAINNAME}
YP Compatibility : OFF
Security Level : 2=DES
```

Is this information correct? {Y or N} **Y**

Use nisclient -r to restore your current network service environment.

Do you want to continue? {Y or N}: **Y**

Enter login password: **{Enter the root password}** <return>

- e. Populate the NIS+ tables from files by executing the following:

```
nispopulate -F -p /etc/nis -d {Enter NIS DOMAINNAME}.
<return>
```

```
Is info correct? y <return>
```

```
Do you want to continue? y <return> (ignore warning on
netgroup)
```

- f. The *nis\_kill* script, executed in Step a, replaces the *nsswitch.nisplus* file with the GCCS version. Consequently, the */etc/nsswitch.conf* file should look like this:

```
passwd: nisplus files
group: files nisplus
hosts: files dns nisplus [NOTFOUND=return]
```

- g. Verify that the NIS+ domain name is correctly set by executing the following:

```
cat /etc/defaultdomain
```

You should see the domain name specified in Step e without the trailing period.

- h. If the NIS+ domain is not correctly set, execute the following:

```
echo {Enter NIS+ DOMAINNAME} > /etc/defaultdomain <return>
```

- I. Reboot the NIS+ server by executing the following:

```
uadmin 2 1 <return>
```

- j. After the system has rebooted, log in as **root** and verify that NIS+ is running by properly executing the following:

1. List all tables in NIS+:  
  
    # **nisls org\_dir** <return>
2. List cache information:  
  
    # **nisshowcache** <return>
3. List user accounts:  
  
    # **niscat passwd.org\_dir** <return>

Verify that all your users are in the *passwd.org\_dir* file and that secman also exists as a user.

- k. Add secman and all other users assigned NIS+ administration duties by executing the following:  
  
    # **nisgrpadm -a admin.** {Enter NIS+ domainname}. {Enter user}. {Enter NIS domainname}. <Return>
- l. After the NIS+ server has been initialized, execute the following as **root**:  
  
    # **nischmod n+r passwd.org\_dir** <return>
- m. You will have rerun the NIS+ client procedures on all other platforms. Section 6.3.3 of this manual should be followed.

## **F.5.2      DNS**

If the DNS database becomes corrupted or the DNS server goes down, the data backed up in */h/USERS/BACKUP/DNS.tar.Z* will have to be used to recover. In the case of a corrupted DNS database you may be able to simply replace the DNS tables in */var/nameserver* to recover (option a). In the case where the DNS server goes down you will have to create a new DNS server (option b).

### **F.5.2.1    Restoring DNS Database on Original DNS Server**

- a. Log on as **root** on the original DNS server and execute the following to kill the DNS processes:  
  
    # **ps -ef | grep named**
- b. Note the process id (pid) and execute the following:  
  
    # **kill -9 {Enter pid}**
- c. Execute the following to extract the backed up DNS database:  
  
    # **zcat /h/USERS/BACKUP/DNS.tar.Z | tar xvf -** <return>

- d. Re-start the name server daemon by executing the following:  

```
in.named <return>
```
- e. Verify that DNS is working correctly by executing the following:  

```
arp {hostname of local platform not in /etc/hosts or NIS+
hosts.org_dir}

arp {fully qualified hostname of platform at another site}
```

In both cases the system should respond with the IP address and Ethernet address of the platform.

#### **F.5.2.2 Building a New DNS Server Using the Backed Up DNS Database**

- a. Log in as **root** on the new DNS server and execute the following:  

```
vi /etc/resolv.conf <return>
```

Change the IP address following *nameserver* to the IP address of the new DNS server.
- b. Execute the following to extract the backed up DNS database:  

```
zcat /h/USERS/BACKUP/DNS.tar.Z | tar xvf - <return>
```
- c. Verify the following files and change the entry for the root DNS server to the hostname of this platform:  

```
/var/nameserver/db.hosts
/var/nameserver/db.rev.hosts
/var/nameserver/db.cache
/var/nameserver/db.local
/var/nameserver/named.boot
```
- d. Execute the following:  

```
cp /var/nameserver/named.boot /etc/named.boot <return>
```
- e. Re-start the name server daemon by executing the following:  

```
in.named <return>
```
- f. Verify that DNS is working correctly by executing the following:  

```
arp {hostname of local platform not in /etc/hosts or NIS+
hosts.org_dir}
```



```
arp {fully qualified hostname of platform at another site}
```

In both cases, the system should respond with the IP address and Ethernet address of the platform.

- g. Log in as **root** on the all other platforms and execute the following:

```
vi /etc/resolv.conf <return>
```

Change the IP address following *nameserver* to the IP address of the new DNS server.

- h. On the secondary DNS servers insure that the IP address of the primary DNS servers are contained in the *db.hosts* and *db.rev.hosts* files.

### **F.5.3 Sybase**

In the event that the Sybase database becomes corrupted, the backup of the GCCS Sybase database and GCCS transaction logs contained in */h/USERS/BACKUP/sybase* can be used to recover (see F.5.3.1). The backup of the GCCS Sybase database and GCCS transaction logs may also be used to build a new Sybase server in the event that the Sybase database server goes down (see F.5.3.2).

#### **F.5.3.1 Restoration of Sybase Database**

-- These procedures are to be delivered later --

#### **F.5.3.2 Rebuilding of Sybase Database Server**

When installing Sybase on a new Sybase server you must create raw partitions or file systems on that system to hold the Sybase database. (See either F.5.3.2.1 or F.5.3.2.2).

##### **F.5.3.2.1 Setting up Sybase Raw Disk Partitions**

If you elect to create the four raw partitions needed by Sybase (standard GCCS configuration) execute the following:

- a. Identify the disk drive you wish to use for Sybase.
- b. De-install anything located on that drive.
- c. Unmount the drive:

Example:

```
umount /home2
```

- d. Execute the **format** command to partition the drive.

- e. Reduce the size of the /home{number} partition by 227MB. Modify slices 3-6 to the values shown in the partition map for a Sybase server (see Appendix B.13).
- f. Label the drive.
- g. Create a file system on the /home{number} partition by executing the following:

```
newfs /dev/rdsk/c0t#d0s1 <return>
```

- h. Mount the /home{number} partition:

Example:

```
mount /home{number} <return>
```

#### **F.5.3.2.2 Setting up Sybase File System**

This procedure is to be used if there are not enough free disk partitions available to use raw partitions.

- a. Identify a partition that has at least 227MB of space available.
- b. Create a directory called *sybase* on this partition:

```
cd {directory}
mkdir sybase
```

- c. Create four files in the *sybase* directory:

```
cd sybase <return>
touch master procs db log <return>
```

#### **F.5.3.2.3 Installing and Initializing Sybase**

- a. Install the Sybase segment using the Segment Installer.
- b. Log in as **root**.
- c. After the install is completed, verify that */etc/system* file has the following entry:

```
set shmsys:shminfo_shmmax=131072000
```

- d. Execute the following:

```
cd /h/COTS/SYBASE/install <return>
vi db_env_setup.MASTER <return>
```

- 1. Change the numbers for the sockets if necessary in the

following lines:

```
setenv SQL_SERVER_PORT 6500
setenv SQL_BACKUP_PORT 6501
```

2. Change the raw partitions in the following lines:

```
setenv MASTER_DEVICE /dev/rdisk/c0t2d0s3
setenv SYSTEMPROCS_DEVICE /dev/rdisk/c0t2d0s4
setenv DB_DEVICE /dev/rdisk/c0t2d0s5
setenv LOG_DEVICE /dev/rdisk/c0t2d0s6
```

If step F.5.3.2.2 (Setting Up Sybase File System) was executed, these lines should look like the following:

```
setenv MASTER_DEVICE {directory}/sybase/master
setenv SYSTEMPROCS_DEVICE {directory}/sybase/procs
setenv DB_DEVICE {directory}/sybase/db
setenv LOG_DEVICE {directory}/sybase/log
```

3. Save the changes as follows:

```
esc
:x<return>
```

4. Execute the following

```
cp db_env_setup.MASTER db_env_setup <return>
./set_partition_permissions <return>
```

Output similar to the following will occur:

```
crw----- 1 sybase sys 32, 3 Feb 23 16:53
/dev/rdisk/c0t2d0s3
crw----- 1 sybase sys 32, 3 Feb 23 16:53
/dev/rdisk/c0t2d0s4
crw----- 1 sybase sys 32, 3 Feb 23 16:53
/dev/rdisk/c0t2d0s5
crw----- 1 sybase sys 32, 3 Feb 23 16:53
/dev/rdisk/c0t2d0s6
```

Or, if file systems are being used instead of raw partitions:

```
crw----- 1 sybase sys 32, 3 Feb 23 16:53
{directory}/sybase/master
crw----- 1 sybase sys 32, 3 Feb 23 16:53
{directory}/sybase/procs
crw----- 1 sybase sys 32, 3 Feb 23 16:53
{directory}/sybase/db
crw----- 1 sybase sys 32, 3 Feb 23 16:53
{directory}/sybase/log
```

5. The System Backup segment places the backup of the GCCS Sybase database in `/h/USERS/BACKUP/sybase`. The following convention is used to label the backup files:

`gccs_dump_{date}_{time}`. To use this backup when initializing Sybase, execute the following:

```
cp /h/COTS/SYBASE/gccs.bak /h/COTS/SYBASE/gccs_bak_orig
<return>
cd /h/USERS/BACKUP/sybase /db_saves<return>
cp gccs_dump_{latest date}_{time} /h/COTS/SYBASE/gccs.bak
<return>
```

6. Execute the following to initialize Sybase:

```
su - sybase <return>
cd install <return>
./install_sybase <return>
```

The output shown in section 11.1g of this manual will be displayed.

7. Set the Sybase System Administrator "sa" password by doing the following:

```
rm -f /h/EM/admin/security-scripts/.sybase_sa <return>
./set_sa_password <return>
```

Enter new "sa" password, then press `<return>`

#### F.5.4 Executive Manager Recovery

In the event that the EM server goes down, another platform must be made into an EM server as rapidly as possible to enable operations to continue. The following procedures will enable you bring a new EM server on line as quickly as possible using the data backed up the *System Backup* segment. It is recommended that the backup EM server be previously identified so that key segments, such as Sybase, can be pre-installed.

##### F.5.4.1 Building a New Executive Manager Server

Execute the following to create a new EM server:

- a. Log in as **root** on the new EM server and do the following:

```
vi /etc/vfstab <return>
```

Remove the following line:

```
emserver:/h/data/global - /h/data/global nfs - yes rw,bg,soft
```

```
vi /etc/dfs/dfstab <return>
```

Add the following line:

```
share -F nfs -o anon=0 /h/data/global
```

```
vi /etc/hosts <return>
```

First, remove the "emserver" alias entry. Then add, the "emserver" alias to line with host name of this platform.

- b. Change the broadcast address in the `/etc/inet/networks` file by executing the following:

```
ifconfig le0 <return>
```

Note the broadcast address:\_\_\_\_\_

```
vi /etc/inet/networks <return>
```

Change the broadcast address shown after "subnet1.gccs" to the address noted above.

- c. Reboot the system by executing the following:

```
uadmin 2 1 <return>
```

- d. Execute the following to make this platform the EM server:

```
/h/EM/systools/EM_make_server <return>
```

- e. Extract the data contained on `/h/data/global` on the original EM server by executing the following:

```
cd /h/USERS/BACKUP <return>
```

```
zcat /h/USERS/BACKUP/GLOBAL.tar.Z | tar xvf - <return>
```

- f. Execute the following to set up global files to recognize new EM server.

```
vi /h/EM/admin/security-scripts/Security_Servers <return>
```

Change host name of old EM server to host name of new EM server.

Example:

```
zeppo:gccs:TRUE:/usr/ucb/rsh:/h/EM/nis_files/
```

```
vi /h/data/global/EMDATA/config/active_spt <return>
```

Change host name of old EM server to host name of new EM server.

Example:

```
u6sysexc#zeppo#System
Executive#/h/EM/progs/uccs_system_executive
```

```
vi /h/data/global/EMDATA/config/processor_table <return>
```

- g. If the EM server is also the NIS+ server (GCCS standard configuration), execute the procedure shown above for building a new NIS+ server (see F.4.3.1.2).
- h. If the EM server is also the Sybase server (recommended), execute the procedure shown above for building a new Sybase server (see F.4.3.3.2).
- i. The report on the segments installed on the original EM server, found in `/h/USERS/BACKUP/local` and titled as `Segments_On_{Hostname}_{date}`, should be consulted. If Netsite, HTTPD, or JNAV server were located on the original EM server, they should be installed immediately.
- j. If the JDISS server segment was installed on the original EM server, it must be installed on this or another platform. Before installing the JDISS server segment, execute the following:

```
vi /etc/inet/hosts <return>
```

Remove the alias `lmserver` and add alias `lmserver` after the host names of this platform.

#### **F.5.4.2 Modifying All Other GCCS Platforms to Use New EM Server**

- a. Execute the following to make other platforms recognize new EM server:

```
vi /etc/inet/hosts <return>
```

Add the IP address of the new EM server and the alias "emserver" after it to the file:

Example:

```
164.117.210.116 emserver
```

- b. `vi /etc/inet/networks <return>`

Change the broadcast address shown after `subnet1.gccs` to the broadcast address of the new EM server as noted above (see F.5.4.1 Step b)

- c. Re-initialize NIS+ on this platform by executing the following:

```
/etc/nis/admin/nis_kill <return>
init 6<return>
```

This kills NIS+ processes and replaces *nsswitch.nisplus* with the GCCS version. It also removes all NIS+ related files/directories (*/etc/.rootkey*, */etc/defaultdomain*, */var/nis*) and changes */etc/nsswitch.conf* to the *nsswitch.files* version.

```
/usr/lib/nis/nisclient -i -d {NIS+ DOMAINNAME} -h {NIS ROOT
SERVER}<return>
```

The following appears on the screen:

```
Enter server (servers name) IP address: {IP Address of
server} <return>
```

```
Please enter the network password that your administrator
gave you. {password} <return>
```

```
Please enter the secure RPC password for root: nisplus
<return>
```

```
Please enter the login password for root: {enter root
password} <return>
```

```
cat /etc/defaultdomain <return>
```

If the NIS+ domain name (without the trailing period) does not appear, execute the following:

```
domainname > /etc/defaultdomain <return>
```

- d. Execute the following to ensure that the */etc/nsswitch.conf* file is properly configured:

```
vi /etc/nsswitch.conf
```

Ensure that the entries for *passwd*, *group*, and *hosts* are exactly as shown below:

```
passwd: nisplus files
group: files nisplus
hosts: files dns nisplus [NOTFOUND=return]
```

- e. Reboot the system by executing the following:

```
uadmin 2 1 <return>
```

- f. Ensure that you can log on to the platform using a user's account.

#### F.5.5 Recovering the Network Installer TOC

Network Installer determines which network segments are available (and which platforms they are installed on) from the */h/data/global/SysAdm/toc\_load* directory. SegDescrip directories for

all available segments are located in this directory. In addition, the file "toc" identifies the location of the segment.

If the `/h/data/global/SysAdm/toc_load` directory is corrupted the network installed will no longer function. To correct this situation execute the following steps:

a.    # `cd /h/data/global` <return>

If the "SysAdm" exists, execute the following:

b.    # `rm -r SysAdm` <return>

Otherwise, extract the table of contents data by entering the following:

```
zcat /h/USERS/BACKUP/GLOBAL.tar.Z | tar xvf -
/h/data/global/SysAdm <return>
```

#### F.5.6 Crash Recovery

Records of the number of instances of *System Backup* that are installed at a site, and the system designated as the tape backup platform, are stored in the `/h/data/global/backup/schedule.ksh` file. This enables the *System Backup* segment to determine when there are no instances of *System Backup* installed at a site or if no system has been identified to do tape backup of `/h/USERS`. If there are no instances of *System Backup* installed at a site, *System Backup* will ask you what time you wish to perform the backup. If no system has been identified to perform a tape backup, the *System Backup* segment will ask you if you wish the platform on which you are installing *System Backup* to perform this function.

If a system crashes and the *System Backup* segment can not be de-installed, `/h/data/global/backup/schedule.ksh` will no longer have the correct information concerning the number of instances of *System Backup* installed and/or the system performing the tape backup. To correct this situation, execute the following command on a system where *System Backup* installed:

```
/h/System_Backup/Scripts/crash_count {Name of platform that
crashed} <return>.
```